UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO
MESTRADO EM MATEMÁTICA

WILLA DA SILVA MEDEIROS

A ARTE DOS CÓDIGOS SECRETOS EM SALA DE AULA: EXPLORANDO CONCEITOS DE MATEMÁTICA BÁSICA EM CRIPTOGRAFIA

MOSSORÓ
2020

WILLA DA SILVA MEDEIROS

A ARTE DOS CÓDIGOS SECRETOS EM SALA DE AULA: EXPLORANDO CONCEITOS DE MATEMÁTICA BÁSICA EM CRIPTOGRAFIA

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Mestre em Matemática do programa PROFMAT.

Orientadora: Prof. Dra. Maria Joseane Felipe Guedes Macêdo

MOSSORÓ

2020

M488a Medeiros, Willa da Silva.
A arte dos códigos secretos em sala de aula: explorando conceitos de matemática básica em criptografia / Willa da Silva Medeiros. - 2020.
162 f. : il.

Orientadora: Maria Joseane Felipe Guedes Macêdo.
Dissertação (Mestrado) - Universidade Federal Rural do Semi-árido, Programa de Pós-graduação em Matemática, 2020.

1. Matemática do ensino básico. 2. Matemática aplicada. 3. Criptografia. I. Macêdo, Maria Joseane Felipe Guedes , orient. II. Título.

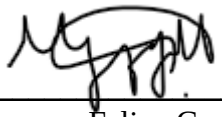
WILLA DA SILVA MEDEIROS

A ARTE DOS CÓDIGOS SECRETOS EM SALA DE AULA: EXPLORANDO CONCEITOS DE MATEMÁTICA BÁSICA EM CRIPTOGRAFIA

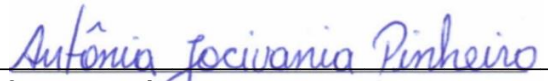
Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Mestre em Matemática do programa PROFMAT.

Defendida em: _25_ / _09_ / 2020

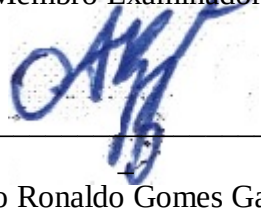
BANCA EXAMINADORA



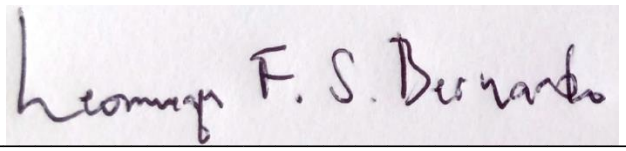
Prof. Dra. Maria Joseane Felipe Guedes Macêdo (UFERSA)
Presidente



Prof. Dra. Antônia Jocivania Pinheiro (UFERSA)
Membro Examinador



Prof. Dr. Antonio Ronaldo Gomes Garcia (UFERSA)
Membro Examinador



Prof. Dr. Leomaques Francisco Silva Bernardo (UFCG)
Membro Examinador (Externo)

À minha mãe Damiana da Silva e demais familiares
À minha esposa Ana Santana Clementino
À minha amada vovó Maria de Lurdes dos Santos
À minha sogra Maria das Graças Clementino

AGRADECIMENTOS

Agradeço a Deus, em primeiro lugar, pelo dom da vida, por me conceder forças, saúde, discernimento e coragem para continuar minha caminhada de estudos, mesmo com todas as dificuldades que a vida nos impõe. A ele sou grato e devo tudo de bom que já me aconteceu, principalmente a oportunidade de realizar mais um sonho.

Sou grato a minha família, nosso bem maior, por todo apoio a me concedido, por todo crédito em mim depositado e por ser a minha principal fonte de inspiração e motivação na vida. Em especial, quero agradecer a minha amada mãe Damiana da Silva, a quem eu devo minha vida, por sempre acreditar no meu potencial e me incentivar nos estudos. Foi muito emocionante realizar o sonho dela de me ver formado e empregado. Quero agora lhe dedicar mais essa conquista e dizer que tudo que fiz, as batalhas que venci, foi tudo por ela.

Sou grato a minha amada esposa Ana Santana, por todo carinho, compreensão e companheirismo de sempre. Agradeço-lhe por todo o incentivo, motivação e por entender o motivo da minha ausência em determinadas ocasiões. Sou imensamente grato a Deus por tê-la ao meu lado durante todos esses anos e por me permitir ser feliz ao lado dela. Este trabalho também é dedicado a ela.

Agradeço de coração a todos os meus amigos colegas e professores do PROFMAT, por toda ajuda concedida durante esses dois anos de mestrado. Em especial, quero destacar os colegas de curso Levi Rodrigo e Auricélio Carneiro. Sem o apoio desses dois amigos, teria sido impossível terminar este curso. Tenho uma dívida eterna com eles e um imenso sentimento de gratidão. Entre os professores, destaco Ronaldo Garcia, Antônio Gomes Nunes, Maria Joseane e Fabrício Figueiredo. Em um momento difícil durante o curso, esses professores, entre outros, foram muito importantes para mim.

Por fim, quero agradecer mais uma vez a minha amiga e orientadora professora Maria Joseane Felipe Guedes Macêdo. A ela sou grato por ter aceitado meu pedido para ser minha orientadora, por toda confiança e credibilidade depositada em mim, por todo tempo, disposição e motivação investidos na orientação deste trabalho e por seu profissionalismo brilhante. Tudo isso foi responsável pelo excelente desenvolvimento e conclusão desta dissertação. Sem dúvidas, o término deste trabalho ocorreu graças à enriquecedora orientação que tive.

Ao final de um trabalho como este, é difícil lembrar-se de todas as pessoas que deram sua parcela de contribuição. Não podendo citar todos, encerro agradecendo todos àqueles que diretamente ou indiretamente contribuíram para a construção deste trabalho.

Muito obrigado!

Por que nos torna tão pouco felizes esta maravilhosa ciência aplicada, que economiza trabalho e torna a vida mais fácil? A resposta é simples: porque ainda não aprendemos a nos servir dela com bom senso.

Albert Einstein (1879 - 1955)

RESUMO

Ensinar matemática não é uma tarefa fácil, pois já é tradição entre os alunos a ideia de que ela é uma disciplina difícil e, em ampla maioria, um amontoado de regras e fórmulas que parecem não possuir nenhuma aplicação prática importante. Neste sentido, é de fundamental importância explorar constantemente as aplicações dos conteúdos de matemática no cotidiano do aluno. Com este intuito, o presente trabalho busca, a partir da criptografia, explorar a relação entre alguns temas de matemática do ensino básico e os métodos criptográficos. Os objetivos principais são: abordar alguns fatos históricos importantes acerca do desenvolvimento dos códigos secretos e da criptografia em geral; relacionar a aritmética básica com um tipo de criptografia muito importante para a segurança na internet hoje em dia, a criptografia RSA; enfatizar como determinados conceitos de matemática podem fazer-se presentes no estudo da criptografia aqui desenvolvido e como isso pode ser útil para o aprendizado do aluno. Este trabalho revela a importância de tratarmos assuntos dessa natureza nas aulas de matemática. Numa época onde a internet torna-se indispensável para o ser humano, é necessário que as pessoas desde cedo conheçam pelo menos as noções mais básicas da inteligência responsável por toda segurança desse veículo de comunicação, a criptografia. Além disso, é de extrema relevância mostrar para os estudantes o papel da matemática na eficiência e no desenvolvimento dessa ciência. Deste modo, foram produzidos alguns algoritmos e guias que servem de apoio ao professor para introduzir e explorar a criptografia como aplicação da matemática em sala de aula.

Palavras chave: Matemática do Ensino Básico. Matemática aplicada. Criptografia.

ABSTTRACT

Teaching mathematics is not an easy task, since it has long been considered, among the vast majority of students, to be a subject full of rules and formulas that seem to have no important practical application. In this sense, it is crucial to constantly explore the applications of mathematical content in students' daily life. For this purpose, the present work seeks, from cryptography, to explore the relationship between some basic mathematics themes and cryptographic methods. The main goals are: to broach some important historical facts concerning the development of secret codes and cryptography in general; to relate basic arithmetic to a type of cryptography that is very important for Internet security today, RSA cryptography; to emphasize how certain concepts of mathematics can be present in the study of cryptography developed here and how it can be useful for student learning. This work reveals the importance of dealing with subjects of this nature in mathematics classes. At a time when the Internet has become indispensable for human beings, it is necessary for people from an early age to know at least the most basic notions of the intelligence responsible for all the security of this communication vehicle, cryptography. Besides, it is extremely important to show students the role of mathematics in the efficiency and development of this science. Thus, some algorithms (guides) were produced that serve to support the teacher to introduce and explore cryptography as an application of mathematics in the classroom.

Keywords: Basic education mathematics. Applied mathematics. Cryptography.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

I INTRODUÇÃO

Recentemente o Brasil passou a integrar o grupo de elite em pesquisa matemática mundial. Somos uma potência em matemática, ao lado de outras grandes potências como Estados Unidos, China, França e Alemanha[1]. Chega a ser espantoso o fato de que essa potencialidade ainda não se refletiu na educação básica. Ainda não conseguimos alcançar patamares mais elevados e o estado atual em que se encontra o ensino e aprendizagem em matemática básica é crítico. Ironicamente, o Brasil é um dos países com pior desempenho em matemática na educação básica como mostra as avaliações educacionais já realizadas. O último PISA (PROGRAMA INTERNACIONAL DE AVALIAÇÃO DE ALUNOS) realizado em 2018 mostrou que apesar de um pequeno aumento na média, o Brasil não conseguiu atingir uma melhoria significativa no desempenho dos estudantes em relação às disciplinas de matemática, português e ciências, ficando entre os 10 países com pior desempenho no ranking mundial[2].

Se tratando de matemática, e de frente a essa real situação, é de extrema importância e urgência a criação e desenvolvimento de práticas inovadoras de ensino e metodologias que possam proporcionar avanços expressivos no ensino e aprendizagem em matemática na educação básica. Nesse conjunto de metodologias, a prática de desenvolver o ensino de matemática por meio da contextualização e interdisciplinaridade dos conteúdos vem se tornando cada vez mais frequente entre os docentes. O ensino de matemática ao ser relacionado com o cotidiano do aluno e com outras ciências torna-se mais prazeroso, produtivo e significativo, pois o aluno pode ver a importância de um determinado conhecimento não apenas dentro da própria disciplina, mas em outras áreas do saber, e isso dá mais sentido ao estudo realizado. Assim, a contextualização e a interdisciplinaridade como forma de apresentar as aplicações da matemática em outros campos são ferramentas poderosas que já vêm sendo bastante usadas no ensino, não só de matemática. Brousseau (1996) citado por Pinheiro (2012) entende que a contextualização ocorre quando o aluno é levado a estudar um conteúdo por meio de uma situação-problema, sendo essa situação próxima à realidade do aluno e, mais ainda, que essa situação esteja inserida num

[1] Ver matéria publicada no site do IMPA (INSTITUTO DE MATEMÁTICA PURA E APLICADA) no dia 27 de fevereiro de 2018. Fonte: <https://impa.br/noticias/tv-escola-destaca-entrada-do-brasil-na-elite-da-matematica/>. Acesso em: 02 jul. 2020.

[2] Ver matéria do G1 em <https://g1.globo.com/educacao/noticia/2019/12/03/brasil-cai-em-ranking-mundial-de-educacao-em-matematica-e-ciencias-e-fica-estagnado-em-leitura.ghtml> e o Relatório Brasil no Pisa 2018 no site do INEP em <http://portal.inep.gov.br/web/guest/acoes-internacionais/pisa/resultados>. Acesso em: 02 jul. 2020.

cenário que seja capaz de atribuir significado e sentido ao objeto de estudo. Desse modo, Brousseau (1996) citado por Pinheiro (2012) deixa claro que dar sentido ao conteúdo ensinado por meio de situações é de extrema importância. Isso se reflete em matemática como resposta àquelas perguntas que todo professor de matemática já ouviu: isso serve para quê? Onde vou usar isso na minha vida?

É nessa perspectiva de contextualização e de inter-relacionar a matemática com outras ciências que o presente trabalho está inserido. A ciência a qual iremos relacionar com a matemática é a criptografia. Uma área da computação muito antiga e que tem sua origem bem parecida com a da matemática. Hoje em dia a matemática é essencial para a criptografia, constituindo sua base conceitual de segurança, assim como também a criptografia é importante para a matemática. A palavra criptografia provém do grego *kriptos*, que significa secreto, oculto, e *graphein*, que significa escrever. Assim, entendemos criptografia como a ciência que estuda os meios, os métodos, para tornar o conteúdo de uma mensagem incompreensível para todos aqueles que não têm permissão de lê-la, de modo que somente o destinatário legítimo possa obter a mensagem verdadeira.

A criptografia está relacionada com muitos conceitos básicos de matemática. Entre eles estão a aritmética básica (fatoração, máximo divisor comum, congruências), as funções (cifras de substituição e criptossistemas em geral), matrizes (cifra de Hill), probabilidades (sigilo perfeito), etc., (BUCHMANN, 2002). Isso faz com que possamos facilmente estabelecer relações entre essas duas áreas nas aulas de matemática. É justamente essa relação que propomos investigar, frisando alguns tópicos de matemática do ensino básico. Sendo a criptografia um tema de enorme relevância, pois representa uma das aplicações mais importantes da matemática para a sociedade, relacioná-la com esses conteúdos tornará as aulas mais interessantes, dinâmicas e consequentemente a aprendizagem mais significativa (PEREIRA, 2015).

Portanto, a relação que pretendemos abordar neste trabalho com a temática envolvendo matemática básica e criptografia é de extremo interesse para o ensino e aprendizagem dessa disciplina. Para Pereira (2015), aspectos da criptografia clássica, como as cifras que iremos tratar no Capítulo 2 já podem ser trabalhados com alunos do ensino fundamental. Essa é uma boa maneira de exercitar operações básicas, noções de análise combinatória, fórmulas matemáticas, raciocínio lógico, resolução de problemas, linguagens, história, etc.

Tópicos de criptografia que envolva a criação de algum algoritmo por meio de computador ou que necessite de um conhecimento de matemática mais aprofundado são aplicações que serão mais bem aproveitadas no ensino médio (PEREIRA, 2015). Ainda em relação ao ensino médio, para Pereira (2015) a abordagem do tema criptografia nessa etapa de ensino será de grande proveito para os alunos, pois possibilitará que os mesmos tomem conhecimento dos conceitos básicos de computação, como desenvolvimento de algoritmos simples, por exemplo, e assim possam compreender melhor o papel da matemática envolvida nesse meio. Isso está de acordo com a BNCC (BASE NACIONAL COMUM CURRICULAR) do ensino médio na habilidade (EM13MAT06)[3]. É claro que muitos dos conceitos e exemplos que veremos serão aplicáveis tanto no ensino fundamental quanto no médio. Entretanto, a relação descrita neste trabalho entre criptografia e matemática destaca com mais evidência conteúdos do ensino médio.

Assim, este trabalho tem por objetivo descrever, por meio de um estudo introdutório, como determinados assuntos de matemática básica (conjuntos, funções, matrizes, probabilidade, análise combinatória, aritmética básica, etc.) estão inseridos em conceitos elementares de criptografia e como isso pode ser útil no aprendizado do aluno. Isso fará com que possamos compreender como esses assuntos podem ser trabalhados, contextualizados, com base no tema criptografia. Os exemplos e as descrições dos métodos (cifras) funcionarão como fonte para desenvolvermos atividades em sala de aula, apesar dessas atividades não serem descritas passo a passo neste trabalho, fornecendo, assim, subsídios para que o professor possa dar maior aplicabilidade aos conteúdos estudados e, com maior ênfase, tornar o estudo mais significativo, sólido e mais próximo da realidade do aluno. Para complementar, abordaremos fatos importantes acerca do desenvolvimento dos códigos secretos e da criptografia, e introduziremos a Criptografia RSA como uma importante aplicação da aritmética básica.

Para o embasamento teórico deste trabalho foram realizadas pesquisas em trabalhos acadêmicos já publicados, tais como monografias, dissertações, artigos e livros que tratam dos tópicos abordados em cada capítulo. Destacamos as obras: Singh (2004), Buchmann (2002), Fiarresga (2010), Brandão (2017), Coutinho (2005), França (2014), Jesus (2013), Santos (2014) e meu TCC da graduação Medeiros (2017). Cada um deles (entre outros) tiveram sua parcela de contribuição no desenvolvimento desta dissertação.

[3] "Utilizar os conceitos básicos de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática" (BRASIL, 2017).

Quanto a sua estrutura, este trabalho está dividido em 3 capítulos, excetuando-se essa introdução e a conclusão. No Capítulo 2 tratamos dos conceitos fundamentais em criptografia. Abordaremos um pouco da sua história, destacando como os primeiros métodos para proteger mensagens enviadas foram criados. Definiremos e exemplificaremos alguns tipos especiais de cifras e finalizaremos o capítulo com uma rápida exposição sobre algoritmos e criptografia de chave pública. O Capítulo 3 trata da aritmética e sua aplicação na criptografia. Nele revisamos alguns conceitos básicos da chamada Teoria Elementar dos Números com a intenção de preparar o terreno para a exposição do método de criptografia de chave pública mais importante atualmente, o RSA. Faremos uma rápida introdução histórica sobre esse método e seus criadores, partindo então para a definição do método e desenvolvimento dos seus processos de codificação e decodificação. Também apresentamos dois algoritmos que servem de guia para introduzir em sala de aula o método RSA. No Capítulo 4 o objetivo é explorar alguns temas de matemática básica em criptografia. Os conteúdos escolhidos, tais como conjuntos, funções, matrizes e probabilidade, são brevemente revisados antes de explicarmos como os mesmos estão inseridos na criptografia. Em suma, estas explicações se resumem em considerar um conceito ou método de criptografia e tratar de discutir como as ideias daquele conteúdo em particular ajudam a entender o funcionamento daquele algoritmo criptográfico simples. Reciprocamente, ao desenvolver as ideias dos métodos criptográficos com base na matemática tratada, teremos mais auxílio para trabalhar melhor a contextualização dos conteúdos com o tema criptografia. Além disso, apresentaremos alguns guias para aplicar tais exemplos em sala de aula.

2 CONCEITOS FUNDAMENTAIS EM CRIPTOGRAFIA

É natural do ser humano a preocupação em impor sigilo a determinadas informações que ele considera importante e que, por algum motivo de privacidade e segurança pessoal não podem ser conhecidas por pessoas não autorizadas. Essa preocupação acompanha o homem desde os tempos mais remotos, sendo ela a responsável pelo desenvolvimento de habilidades extraordinárias para manter a segurança das informações trocadas via mensagens.

A troca de mensagens representou um grande avanço no desenvolvimento da comunicação, possibilitando o tráfego dessas informações por vias de diferentes naturezas. No entanto, durante um intercambio de mensagens, onde o conteúdo das mesmas não poderia ser compartilhado por pessoas não autorizadas, o emissor e o receptor (quem envia e recebe a mensagem, respectivamente) tinham ciência do perigo caso tal mensagem chegasse a mãos erradas. Assim, entra em cena a questão da segurança e privacidade dessas mensagens: como enviar uma informação sigilosa com segurança de modo que, se por ventura ela caia em mãos inimigas, seu conteúdo não possa ser compreendido?

Tal pergunta, e o problema central que a acompanha, foram responsáveis por fazer com que o homem desenvolvesse técnicas de proteção e ocultação do significado real de uma mensagem antes da mesma ser *enviada* para outra pessoa. Dessa maneira, o envio e, principalmente, o trajeto dessa mensagem se tornam mais seguros e com maior probabilidade de não ser violados. Surgem então os códigos secretos, os procedimentos, e os algoritmos para proteger as comunicações.

Com a evolução das comunicações e o desenvolvimento da linguagem, os códigos tiveram que ser aperfeiçoados, se não substituídos, para poder atender a crescente demanda por segurança no envio de mensagens. A evolução dos códigos primitivos se dar com o surgimento das *cifras* (explicaremos adiante o que isso significa) que, segundo Singh (2004), dominaram a arte dos códigos secretos no primeiro milênio. Porém, estas cifras não conseguiram seguir no topo da segurança das comunicações. Isso porque havia outro ramo de estudo, chamado criptoanálise, que se destinava a desenvolver alternativas para vencer as cifras. Isso fez com que fossem idealizados vários tipos de cifras com o intuito de aperfeiçoar as alterações feitas nas mensagens. Mesmo assim, estas cifras eram baseadas em métodos que possuíam muitas deficiências quanto ao seu modo de mudar o significado de uma mensagem e a maneira de recuperá-la. Essa deficiência foi responsável por fazer com que um novo ramo de escrita secreta surgisse. Daí em diante a escrita secreta toma um novo rumo, mais

moderno, onde a matemática desempenha o papel principal, garantindo a segurança dos códigos.

Hoje, conhecemos o estudo da arte dos códigos através da criptografia, uma ciência que se encarrega de desenvolver métodos que possibilitem o máximo de privacidade e segurança no envio de mensagens.

O objetivo principal deste capítulo é deixar o leitor a par dos conceitos básicos mais importantes sobre criptografia, e fazer uma contextualização histórica de como se deu o surgimento dos métodos criptográficos clássicos, as cifras clássicas. Para isso, iniciaremos falando um pouco sobre a origem dos códigos. Abordaremos um pouco de história das cifras como parte importante no desenvolvimento da criptografia, destacando alguns exemplos de cifras muito utilizadas no passado. Abordaremos conceitos de extrema importância em criptografia, tais como codificação, decodificação, criptografia de chave pública, criptografia de chave privada, etc. Por fim, trataremos da "inimiga" da criptografia: a criptoanálise. A criptoanálise estuda os métodos pelos quais se podem vencer os algoritmos criptográficos, isto é, ela busca desenvolver técnicas que sejam capazes de descobrir o texto original de uma mensagem codificada. Precisamente, ela tentar "quebrar" os códigos propostos pela criptografia. Os conceitos básicos aqui apresentados são de fundamental importância para o bom entendimento deste texto. Sem tal conhecimento é difícil apreciar esta belíssima ciência e, principalmente, será difícil apreciar o trabalho aqui realizado.

2.1 Sobre a Origem dos Códigos Secretos

2.1.1 Um relato devido a Heródoto[4]

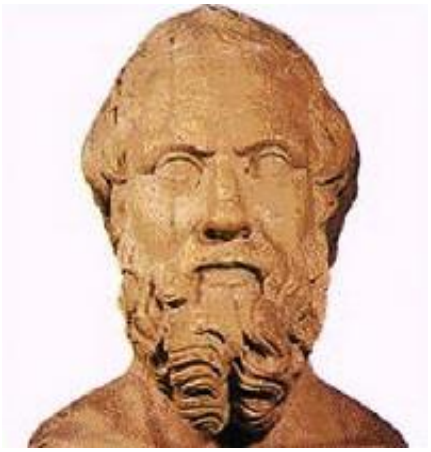
Precisar quando os códigos secretos surgiram é algo muito complicado, pois há inúmeros relatos da utilização de códigos em envios de mensagens em épocas remotas e em períodos diferentes da história da humanidade. Acredita-se, e seria o natural a supor com base nos relatos históricos, que os primeiros procedimentos para ocultar a existência de uma mensagem ao ser enviada surgiram com maior evidência no período das grandes guerras ocorridas há milhares de anos. De fato, "durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus

[4] Historiador e geógrafo grego. Viveu entre 485 a.C e 425 a.C.
Fonte: <https://pt.wikipedia.org/wiki/Her%C3%B3doto>. Acesso em: 28 set. 2019

exércitos" (SINGH, 2004, p.11). Essa dependência de uma comunicação mais segura provocou o início da era dos códigos secretos. "Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler seu conteúdo" (SINGH, 2004, p. 11).

No primeiro capítulo de Singh (2004) consta que um dos primeiros relatos relacionados à utilização de escritas secretas se deve ao grande historiador Heródoto, conhecido como o pai da história.

Figura 1 – Heródoto



Fonte: <https://images.app.goo.gl/6Dcu5Aq4d4enZZij9>

Acesso em: 25 set. 2019

Nesse contexto, Besselaar (1962) ainda nos situa no ambiente no qual se desenvolveu todo o trabalho de Heródoto. O autor comenta:

> Heródoto viveu, globalmente falando, entre os dois grandes conflitos do povo grego no século V, entre as guerras persas e as guerras do Peloponeso, isto é, numa Grécia vitoriosa sobre os bárbaros e cheia de si, numa Grécia dolorosamente dividida por correntes de separatismo e por tentativas de imperialismo, mas numa Grécia ainda não dilacerada, massacrada e humilhada. Neste ambiente viveu e respirou Heródoto, deste ambiente sua obra é a eloquente expressão [...]. (BESSELAAR 1962, p. 7)

Nesse ambiente, Heródoto narra um episódio sobre os conflitos entre a Grécia e a Pércia ainda no século V a.C. onde se observa a utilização de uma manobra para enviar uma

mensagem secretamente. Para entender como tudo se originou devemos nos ater as palavras de Singh (2004), que nos diz:

> A antiga inimizade entre a Grécia e a Pércia evoluiu para uma crise logo depois que Xerxes começou a construir a cidade de Persépolis, a nova capital do seu reino. Presentes e tributos chegaram de todas as regiões do império e dos estados vizinhos, com a notável exceção de Atenas e Esparta. Determinado a vingar esta insolência, Xerxes começou a mobilizar um exército [...]. Ele passou os cinco anos seguintes montando secretamente a maior força de combate da história. Então, no ano 480 a.C., ele estava pronto para lançar um ataque-surpresa. (SINGH, 2004, p. 20)

Xerxes é o rei, líder dos persas. No entanto, ao elaborar seu ataque ao povo grego, ele não imaginava que seus planos estavam sendo observados por outra pessoa que não era seu aliado. Esta outra pessoa se chamava Demarato[5], um grego que mesmo depois de ser expulso da Grécia ainda era fiel ao seu país de origem e estava disposto a tudo para salva sua terra natal do terrível ataque do exército persa. Havia, entretanto, um problema: como fazer para avisar os gregos sobre o ataque de Xerxes? Segundo Heródoto, citado por Singh (2004):

> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mesma foi coberta novamente com cera. Deste modo, as tabuletas pareciam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isso foi feito, revelando a mensagem, então transmitida para os gregos.

Com isso, graças à engenhosidade de Demarato, os Gregos tiveram condições de se preparar para o ataque de Xerxes, se armando fortemente para tal fim. Assim, ainda segundo Singh (2004), com a perda do elemento surpresa, o rei Xerxes e todo o seu exército foram surpreendidos e encurralados na baía de Salamina, aos arredores de Atenas, perdendo o confronto humilhantemente para o exército grego. Graças a uma escrita secreta, os gregos foram capazes de se livrar dos Persas e vencer a guerra.

O relato feito acima por Heródoto citado por Singh (2004) representa um dos primeiros que trata da utilização de um método primitivo para mascarar a existência de uma mensagem. Veja que Demarato se preocupou em esconder a mensagem, e não seu conteúdo. Este tipo de estratégia era muito comum e foi a primeira a ser utilizada pelo ser humano para

[5] Grego, rei euripôntida de Esparta (Cidade – Estado da Grécia antiga) que viveu entre 515 a.C e 491 a.C. Fonte: <https://pt.wikipedia.org/wiki/Demarato>. Acesso em: 28 set. 2019

esconder os vestígios de suas comunicações secretas. Na seção seguinte, este tipo de estratégia receberá um nome especial, e passaremos a discuti-la com mais alguns exemplos.

2.1.2 Esteganografia e Criptografia

Como falamos anteriormente, sobre a estratégia de Demarato, a sua ideia foi esconder a mensagem nas tabuletas de madeira raspando sua cera. Quando usamos algum meio para esconder a mensagem em nossas comunicações, estamos praticando a esteganografia. Mais precisamente, temos que "a comunicação secreta, quando é obtida através da ocultação da mensagem, é conhecida como esteganografia, nome derivado das palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever" (SINGH, 2004, p. 21). Portanto, podemos entender esteganografia como a ciência que busca criar meios, métodos, que possibilitam manter a existência de uma mensagem em total segredo quando a mesma é enviada ao seu destinatário.

Ainda se tratando de Heródoto, o mesmo detalhou mais um episódio onde se utilizou a comunicação por meio da ocultação da mensagem, ou seja, a esteganografia, para repassar uma informação secreta. Ele narra a história de Histaeu (515 a.C – 493 a.C)[6], que queria fazer com que Aristágora de Mileto[7] se revoltasse contra o rei persa Dário I. A estratégia de Histaeu é ainda mais inusitada do que a de Demarato. Singh (2004) nos conta qual foi essa estratégia:

> Para transmitir suas informações em segurança, Histaeu raspou a cabeça do mensageiro, escreveu a mensagem no couro cabeludo e esperou que o cabelo voltasse a crescer. O mensageiro, que aparentemente não levava nada que fosse perigoso, pôde viajar sem ser incomodado. Quando chegou ao seu destino, raspou a cabeça e a virou para o destinatário da mensagem. (SINGH, 2004, p. 21)

Logicamente, tal método é bem utilizado quando a mensagem não é urgente, em vista de ter que esperar o cabelo crescer. No entanto, ele é um belo exemplo de como o ser humano foi capaz de pensar em variados tipos de métodos de esteganografia para poder enviar suas mensagens em segurança. Outro episódio devido a Heródoto é, segundo Julio *et al*. (2007, p. 57), o caso de um mensageiro que pretendia entregar, secretamente, uma determinada mensagem ao rei. O mensageiro, então, tem a ideia de se passar por um caçador, onde,

---

[6] Tirano de Mileto sob o governo do rei persa Dário I.
Fonte: <http://www.historyofwar.org/articles/people_histiaeus.html>. Acesso em: 24 out. 2019.

[7] Líder de Mileto no período que abrange o fim do século VI a.C e o início do século V a.C. Era genro e primo de Histaeu. Fonte: <https://pt.wikipedia.org/wiki/Arist%C3%A1goras>. Acesso em: 24 out. 2019.

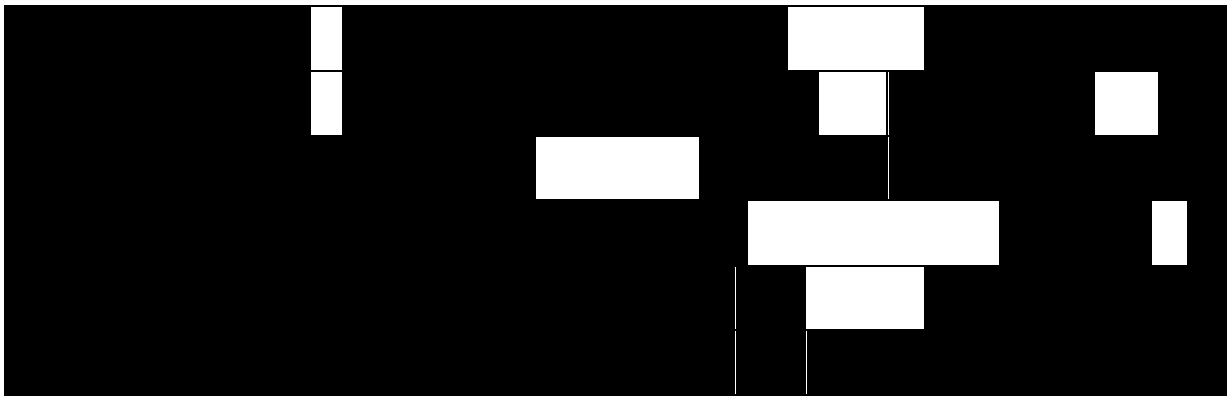
colocando a mensagem dentro de uma lebre, pôde passar livremente pelos guardas sem ser incomodado.

Além dos exemplos de esteganografia dados por Heródoto, muitos outros foram surgindo ao longo dos anos que sucederam a morte deste historiador. Um deles é devido ao povo chinês. Segundo Singh (2004), para esconder uma mensagem os chineses a escrevia numa seda fina que era então amassada em formato de bolinha e envolvida numa cera. Para o transporte dessa mensagem, o mensageiro a engolia, escondendo assim sua existência.

Outro exemplo de esteganografia vem do povo grego. Na Grécia antiga se desenvolveu um meio para enviar mensagens escondidas em livros. O método consistia em furar buracos acima das letras que formavam a mensagem. Assim, quando o livro estivesse nas mãos do destinatário, o mesmo buscaria pelos furos no texto e reescreveria novamente a mensagem enviada. É claro que tal método é muito frágil e fácil de ser violado. Se uma pessoa muito esperta suspeitasse do código, poderia fuçar o livro à procura dos furos e, consequentemente, tomaria conhecimento da mensagem.

Ainda se tratando de exemplos de esteganografia, o próximo método é devido ao matemático italiano Girolamo Cardano (1501 - 1576). Tal método é conhecido como *grade de Cardano (ou grelha de Cardano*). Este método se utiliza de uma folha rígida, chamada lâmina, na qual constam vários furos retangulares aleatórios, isto é, tais furos têm tamanhos aleatórios e são espaçados de modos distintos, com alturas mais ou menos igual à de uma linha de texto. Para utilizar este método, coloca-se a grade sobre uma folha de papel de mesmas dimensões e escrevem-se as palavras da mensagem nos retângulos formados. Depois disso, os espaços que sobram em branco são preenchidos com outras palavras ou letras quaisquer de modo a formar a mensagem total que seria enviada, isto é, a “mensagem de cobertura” (JULIO et al., 2007, p.58). Para recuperar a mensagem, o destinatário utiliza uma grade idêntica àquela utilizada pelo remetente para escrever a mensagem. Ele coloca sua grade sobre o texto, a qual revela a mensagem enviada.

Figura 2 – Um exemplo de Grade de Cardano



Fonte: autoria própria

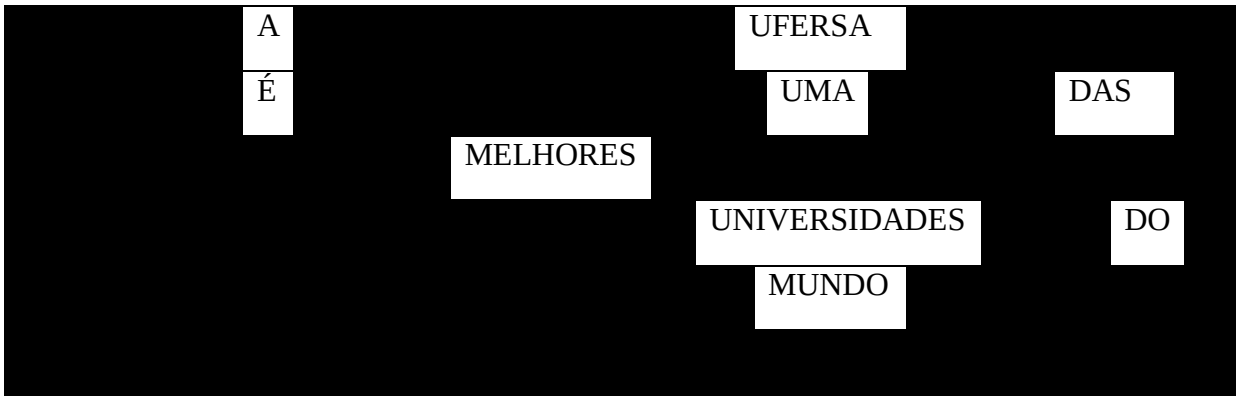
Figura 3 – Mensagem de Cobertura

ANDREJSKDXBHCBACRIPTOGRAFIAOKFSHGHYUSYUFERSAMÉTODOSMATEEJ
WIJAAHDGSBDTEEIÉHIEUMATEMÁTICAHFHDJHJJDSIUMAGHDUASDHSDASLO
JJHDHJAAUDDHGCIFRASJWHJWWMELHORESLIVROCÓDIGOSTRYKJAJJDHSQP
VBSIALKFGTSEJSUDHHAGDNSLUEDQPOALAJDHUNIVERSIDADESEVATSDDOK
DISGFAJHAJSERTAHFJDFHCAOHSWUUIURMATHERHMUNDOCONCLUSAOWYE
AGORADLSKKJRIRJKDVAMOSJIREIURSNFJHJKFHESTUDARKFKJGKLWOIRUUS

Fonte: autoria própria

Na Figura 2 temos um exemplo de uma grade de Cardano e na Figura 3 um exemplo de mensagem de cobertura. Para conseguirmos identificar a mensagem secreta é preciso que coloquemos sobre a mensagem de cobertura uma grade idêntica à apresentada na Figura 2. A Figura 4 a seguir ilustra este procedimento.

Figura 4 – Decifrando a mensagem



Fonte: autoria própria

Ao fazemos isso, surgirá a mensagem:

A UFERSA É UMA DAS MELHORES UNIVERSIDADES DO MUNDO

Outro método muito conhecido de esteganografia, bastante usado na primeira e segunda guerra mundial, é o *microponto***.** A ideia do microponto era, segundo Singh (2004), reduzir uma mensagem, ou uma página de texto como o autor sugere, fotograficamente até que a mesma tomasse a forma de um minúsculo ponto. Feito isso, tal mensagem poderia se passar por um ponto final em uma frase qualquer do texto ou por um pingo em um "i" de alguma palavra. Ainda segundo o autor, foi na segunda guerra mundial que este método se tornou realmente popular, sendo um dos métodos preferidos dos alemães para enviar suas mensagens secretas.

Finalmente, a esteganografia também aborda os métodos de ocultação de mensagens através da utilização das chamadas tintas invisíveis. Tal método é muito antigo e consiste basicamente na utilização de substâncias extraídas de plantas, fluidos orgânicos, entre outros, que se comportam de maneira a ficar transparentes depois de secas, mas voltam a aparecer depois de um aquecimento do material na qual elas foram aplicadas. A este respeito, Singh (2004, p.22) ressalta que "no primeiro século depois de Cristo, Plínio, o velho, já explicava como o 'leite' da planta titímalo podia ser usado como tinta invisível. Embora fique transparente depois de seca, um aquecimento suave queima a tinta, tornando-a marrom". Neste caso, para mandar uma mensagem secreta, bastaria escrevê-la em uma folha com o leite da titímalo e esperar que o mesmo secasse. Depois de seco, o texto desaparecia e a mensagem

poderia ser enviada em segurança. Ao chegar ao destinatário, um simples aquecimento na folha poderia revelar o conteúdo da mensagem.

Os métodos de esteganografia foram por muito tempo a melhor opção para se enviar uma mensagem em segurança. No entanto, os exemplos anteriores nos mostram que esta segurança carece de potencial. Isto é, essa segurança é relativa, uma vez que se o meio pelo o qual a mensagem está sendo transportado, digamos, um mensageiro, seja interceptado, a mensagem pode ser facilmente achada (já que ela está escondida!). Com respeito a este fato, Singh (2004) reitera o que acabamos de falar:

> A interceptação da mensagem compromete toda a sua segurança. Uma vigilância rígida pode revistar qualquer pessoa que cruze a fronteira, raspando a cera de qualquer tabuleta, aquecendo folhas de papel em branco, [...] raspando a cabeça das pessoas. E assim, inevitavelmente, haverá ocasiões em que a mensagem será descoberta. (SINGH, 2004, p. 22)

Assim, embora a mensagem estivesse oculta e isso representasse certa segurança, era necessário algo mais. Para impor um alto nível de segurança nos envios de informações privadas, não bastaria apenas fazer com que essa informação desaparecesse. Era preciso que além da anulação visível, fosse desenvolvido algum meio para tornar o conhecimento da informação, por parte de terceiros não autorizados, mais difícil.

Métodos e alternativas para modificar o texto original de uma mensagem, tornando-o ilegível para aqueles que não fossem seu real destinatário, impulsionaram o desenvolvimento de uma das mais importantes ciências do século XX, e do século XXI com maior evidência, chamada *criptografia*. A palavra criptografia vem do grego *kriptos*, que significa secreto, oculto, e *graphein*, que significa escrever. Assim, podemos entender criptografia como a ciência que estuda os meios, os métodos, para tornar ilegível o significado original de uma mensagem, de modo que somente o receptor verdadeiro tenha possibilidade de lê-la. De acordo com Singh (2004), a criptografia não se interessa em esconder a mensagem. Ela está preocupada, como a definição acima mostra, em dificultar a compreensão do texto original para intrusos[8]. Para isso, tanto o emissor quanto o receptor utilizam um processo lógico para

[8] Usaremos frequentemente os termos *intruso, inimigo,* para se referir a um indivíduo que tenta quebrar um código, ou seja, que não tem a chave de decodificação. Tal indivíduo não possui permissão para participar da comunicação via mensagens, mas tenta interferir de algum modo. Esses termos, intruso, inimigo, ou ainda criptoanalista, são clássicos em textos de criptografia. Por isso iremos permanecer com sua utilização, apesar de que o significado preciso dessas palavras nem sempre vão condizer com a intenção do indivíduo que tentar quebrar um código. Por exemplo, se um grupo de inteligência tenta grampear a comunicação de terroristas para o bem da população, esse grupo só é inimigo com relação aos terroristas.

poder se comunicar. O transmissor utiliza um método chamado *codificação*, ou *encriptaçã*o, para modificar o conteúdo original da mensagem. O receptor recupera a mensagem através da *decodificação*, ou *descriptação*. Tanto a codificação quanto a decodificação são processos que constituem um "protocolo específico, que já foi estabelecido previamente por ambos, transmissor e receptor" (SINGH, 2004, p. 22). De modo intuitivo, significa combinar como será feito a mudança no texto original da mensagem e quais passos seguir para reverter esse processo e recuperar a forma original dessa mensagem. Posteriormente, vamos nos referir a este protocolo como um método criptográfico ou criptossistema. Definiremos estas noções quando oportuno.

2.1.3 Cifras de Transposição e Substituição

Quanto a sua estrutura, a criptografia pode ser dividida em dois ramos que, segundo Singh (2004), são denominados *transposição* e *substituição*. O que é um método de transposição em criptografia? Transpor é sinônimo de permutar. Portanto, os métodos de transposição consistem simplesmente em permutar, rearranjar as letras que constituem a mensagem. Se considerarmos uma mensagem muito curta, digamos com uma palavra somente, então fica muito fácil decodificar a mensagem, pois haverá um número relativamente pequeno de rearranjos para checarmos. Por exemplo, observe que a palavra PROFMAT tem 7 letras, então da análise combinatória, ela admite 7! (7 fatorial) permutações de suas letras (anagramas) (Ver Capítulo 4, Seção 4.1.5). Isso quer dizer que há 7! maneiras, distintas, já que as 7 letras são diferentes, de codificar a palavra PROFMAT por meio da transposição. O número 7! = 5040 é pequeno e se tivermos a disposição um computador, ficará fácil descobrir todos os anagramas. É claro que quando estes métodos surgiram não havia nem a ideia de uma máquina parecida com o computador, de modo que os métodos de transposição foram bastante usados e considerados bem eficientes para a tecnologia da época. Entretanto, palavras curtas não estavam totalmente isentas de serem descobertas pelo método de checagem de todos os anagramas, mesmo que demorasse muito tempo.

Se com palavras pequenas este método é frágil, seria ele totalmente seguro para frases longas? Não necessariamente. Singh (2004, p. 23) esclarece que:

> [...] à medida que o número de letras aumenta, o número de arranjos possíveis rapidamente explode, tornando impossível obter-se a mensagem original [...]. Mas há uma desvantagem. A transposição efetivamente gera um anagrama incrivelmente difícil e, se as letras forem misturadas ao acaso, sem rima ou fundamento, a

> decodificação do anagrama se tornará impossível, tanto para o destinatário quanto para o interceptador inimigo. (SINGH, 2004, p. 23)

Quer dizer que, se não há um protocolo bem estabelecido entre o transmissor e o receptor, então este tipo de método criptográfico é inviável nas trocas de mensagens. A permutação não pode ser aleatória, como deixa claro o autor. Pense, por exemplo, em uma frase como "*Criptografia é a arte dos códigos secretos"*. Ela possui 36 letras e mais de 500 000 000 000 000 000 000 000 (quinhentos sextilhões) de rearranjos distintos possíveis. Logo, inviável para qualquer pessoa testar cada um desses rearranjos. Portanto, para resolver este problema, basta o transmissor e o receptor combinarem qual o processo lógico que será utilizado para codificar a mensagem. Tal processo, claro, não pode ser conhecido por pessoas não autorizadas.

O exemplo abaixo trata de uma maneira bem simples de transposição e foi extraído de Singh (2004). O método consiste em escrever uma mensagem qualquer distribuindo as letras que a formam em duas linhas paralelas de modo que tais letras fiquem alternadas nestas linhas. Assim, a primeira letra fica, digamos, na linha de cima, a segunda letra fica na linha de baixo, a terceira letra fica na linha de cima, e assim por diante. Considere a frase a seguir:

TEU SEGREDO É TEU PRISIONEIRO; SE DEIXÁ-LO PARTIR SERÁ PRISIONEIRO DELE.

Agora desconsiderando os espaços entre palavras, as pontuações e os acentos, podemos reescrever esta mensagem assim:

TEUSEGREDOETEUPRISIONEIROSEDEIXALOPARTIRSERAPRISIONEIRODELE

Pelo método de transposição que descrevemos acima, esta mensagem fica assim:

T U E R D E E P I I N I O E E X L P R I S R S R S O E R D L
E S G E O T U R S O E R S D I A O A T R E A P I I N I O E E

A mensagem codificada é, então, representada pela sequência de letras da linha superior seguida da sequência de letras da linha inferior, como segue:

TUERDEEPIINIOEEXLPRISRSRSOERDLESGEOTURSOERSDIAOATREAPIINIOEE

Para recuperar a mensagem, o receptor deverá refazer os passos em ordem contrária. Tal método é denominado "cerca de ferrovia" (SINGH, 2004, p. 24).

Ainda no século V a.C., o exército espartano foi o responsável por idealizar uma forma bem inteligente de enviar mensagens codificadas por transposição através de um aparelho chamado de *Citale*. O Citale tem formato cilíndrico, assemelhando-se a um pequeno bastão, que pode ser de madeira ou de outro material qualquer (naquela época estes aparelhos eram feitos de madeira), no qual era enrolada uma fina tira de pano, ou couro, de modo que as faixas de tiras não ficassem sobrepostas. Para codificar uma mensagem através deste aparelho, o emissor a escrevia ao longo da linha do comprimento do Citale. Quando a tira era desenrolada, o que se via era apenas um monte de letrinhas espalhadas, sem sentido e sem ordem. Ao chegar ao seu destino, a mensagem só era revelada se a tira fosse colocada sobre outro Citale com as mesmas dimensões daquele que foi usado para codificá-la.

Para qualquer intruso que por ventura interceptasse o mensageiro, mesmo que a mensagem fosse capturada, era preciso ter em posse um Citale idêntico ao utilizado pelo emissor. Caso contrário, a mensagem permaneceria em segredo. Dependendo da esperteza do mensageiro, ele poderia se utilizar da esteganografia e tentar esconder a tira com as letras em algum lugar em seu corpo para aumentar a segurança no envio (por exemplo, poderia usar a tira como um cinto ou amarrá-la na perna por debaixo das roupas). O Citale espartano, como é conhecido hoje, foi, segundo Singh (2004), o primeiro aparelho de criptografia militar utilizado. O Citale também é conhecido por *Scytale* ou *Bastão de Licurgo*. "A sua referência encontra-se descrita no tomo III de As Vidas Paralelas de Plutarco" (FIARRESGA, 2010, p.7), que é um conjunto de obras bibliográficas dos ilustres homens da Roma e Grécia antigas escritas por Plutarco[9]. Na figura abaixo, ilustramos um exemplo de Citale.

Figura 5 – Citale ou Bastão de Licurgo

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

Acesso: 18 set. 2019

[9] Lucius Mestrius Plutarchus (46 d.C. – 120 d.C, aproximadamente). Foi historiador, filósofo e biógrafo grego. Fonte: <https://pt.wikipedia.org/wiki/Plutarco>. Acesso em: 18 set. 2019.

Alternativamente, também temos os métodos de Substituição em criptografia. Ao contrário do que ocorre com a transposição, onde mudamos a posição das letras, mas estas conservam suas identidades, nos métodos de substituição cada letra na frase será substituída por outra letra, mas a posição dessa letra não é alterada. Por exemplo, poderíamos utilizar um processo de codificação que consiste em substituir cada letra do nosso alfabeto original A, B, C, D, E, ..., pela letra seguinte. Assim, o A seria substituído pelo B, o B passaria a ser o C e assim sucessivamente. Logo, se quiséssemos mandar a mensagem **volto ao amanhecer** por meio desse método, então depois de codificada, esta mensagem passaria a ser **WPMUP BP BNBOIFDFS.** Veja que nenhuma letra da mensagem mudou de posição, isto é, o V continua sendo a primeira letra na frase, o O a segunda, o L a terceira e assim por diante. Mas a identidade destas letras mudou. Na mensagem codificada, o V passa a ser o W, o O passa a ser o P, *etc*.

Na criptologia[10], qualquer método que consiste em substituir uma letra do alfabeto original, a qual consta na mensagem, por outra letra ou símbolo é chamado de *Cifra*. Deste modo, podemos nos referir aos métodos de codificação por substituição como cifras de substituição. Assim, os métodos de transposição serão chamados de cifras de transposição. Esta linguagem é mais adequada e mais usada na literatura. Passaremos a usar esses termos com mais frequência a partir de agora.

Segundo Singh (2004), um dos primeiros exemplos de Cifras de substituição que foi descrito na literatura apareceu num livro muito antigo, escrito ainda no século IV, chamado *Kama-Sutra*. Segundo o autor:

> O Kama-Sutra recomenda que as mulheres devem estudar 64 artes, incluindo culinária, vestuário, massagem e preparação de perfumes. A lista também inclui algumas artes menos óbvias, incluindo magia, xadrez, encadernação de livros e carpintaria. O número 45 da lista é a mlecchita-vikalpa, a arte da escrita secreta, justificada de modo a ajudar as mulheres a esconderem os detalhes de seus relacionamentos. (SINGH, 2004, p. 25)

Uma das Cifras apresentada no Kama-Sutra, de acordo com Singh (2004), consistia numa técnica simples que era a seguinte: considerando nosso alfabeto original, no qual há 26 letras, separe de modo aleatório essas 26 letras em dois grupos de 13 letras. Agora coloque

[10] "É a ciência da escrita secreta em todas as suas formas, cobrindo ambas, a criptografia e a criptoanálise" (SINGH, 2004, p. 424).

esses dois grupos em duas linhas paralelas de modo que as letras fiquem em correspondência uma a uma, como na Tabela 1 a seguir.

Tabela 1 – Cifra do tipo citado no Kama-Sutra

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

Fonte: Autoria própria

Assim sendo, cada letra na mensagem será substituída por àquela que lhe é correspondente na tabela acima. Assim, por exemplo, a palavra **Matemática** codificada passaria a ser **WCBNWCBJAC.** Note que na tabela que apresentamos anteriormente, temos apenas uma das inúmeras maneiras de montá-la, usando o raciocínio de montar dois grupos de 13 letras, de modo que fica muito difícil para um invasor descobrir como a mensagem foi codificada**,** pois existe um número imenso de modos distintos de se fazer isso. Só por curiosidade, há $\binom{26}{13}$ maneiras distintas de montar a tabela acima, isto é, há $\binom{26}{13}$ maneiras distintas de codificar uma mensagem qualquer por meio dessa Cifra. O número $\binom{26}{13}$ é o binomial de 26 tomados 13 à 13, e o mesmo é igual a $\frac{26!}{13!(26-13)!}$.

Neste caso, dizemos que a cifra destacada acima transforma o nosso *alfabeto usual* (ou *alfabeto original*) A, B, C, D, E, F, G, H, ... Y, Z no *alfabeto cifrado* C, T, A, X, N, H, P, F,..., L, S. O alfabeto original é aquele que utilizamos para escrever a mensagem de modo correto, legível. Já o alfabeto cifrado é aquele composto pelas letras, ou símbolos, que serão usados para codificar uma mensagem.

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

Na linguagem da criptografia é comum escrevermos o alfabeto original em minúsculo e o alfabeto cifrado em maiúsculo. Assim, as mensagens que apresentaremos cifradas serão escritas em maiúsculas, enquanto que as mensagens originais a elas correspondentes serão dadas em minúsculas (SINGH, 2004).

Voltando ao exemplo dado acima sobre a cifra apresentada no Kama-Sutra segundo Singh (2004), veja que dentre tantas possibilidades para montarmos o alfabeto cifrado,

poderíamos pensar naquelas que consistem em substituir cada letra do alfabeto original por outra letra que está a uma distância de uma, duas,..., ou 25 letras desta. Este tipo de cifra de substituição é muito antigo e é considerado um dos primeiros a ser usado para fins militares em guerras. Neste ambiente de conflitos militares, o imperador romano *Julio César* (100 a.C – 44 a.C)[11] foi o primeiro a usufruir deste tipo de cifra para se comunicar com seu exército em combate. De acordo com Singh (2004), a ideia inicial de César foi substituir cada letra do alfabeto original por aquela que estivesse a três casas desta letra. Assim, por exemplo, o A seria substituído pelo D, o B seria substituído pelo E, o C passaria a ser o F, e assim por diante. Então, a palavra *código*, cifrada, passaria a ser FRGLJR. O alfabeto cifrado seria, então, o seguinte:

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

Veja que ele nada mais é do que o alfabeto original, transladado três casas à frente. É claro que não há nada de especial em escolher três casas para transladar o alfabeto. Poderia ser uma escolha qualquer entre 1 e 25 (26 casas não dar, pois voltaria para a mesma letra). Logo, o alfabeto original pode ser transladado de 25 maneiras e cada uma dessas maneiras dará origem a uma cifra do tipo acima. Em homenagem ao imperador Julio César, estas cifras são conhecidas como *cifras de César*.

Um caso particular muito interessante da cifra de César é a chamada cifra ROT-13. Ela consiste em transladar o alfabeto 13 casas à frente. Neste caso, o A será substituído pelo N, o B pelo O e assim por diante. É claro que a letra N será substituída pela letra A, a letra O passará a ser o B, *etc*., numa rotação característica das cifras de César, daí a sigla ROT-13 (que deriva de *rotate by 13 places*, que significa girar 13 lugares, isto é, rotacionar 13 posições). Quanto à segurança dessa cifra, trata-se da mesma segurança das cifras de César, isto é, baixa e de fácil violação, pois para reverter o processo de codificação basta saber quantas letras o alfabeto foi deslocado. Mesmo assim, ela se destaca no meio computacional, como afirma Freitas *et al*. (2018):

> [...] a cifra de ROT-13, aplicada aproximadamente em 1980 na USENET, era utilizada para ocultar piadas politicamente incorretas, ou spoilers. Números, espaços e pontuação não são alterados. É usada principalmente para proteger endereços de

[11] Conheça um pouco da história de César em: < https://www.ebiografia.com/julio_cesar/>. Acesso em: 27 out. 2019.

> correio eletrônico, e também mensagens postadas em grupos e listas de discussão online. (FREITAS et al., 2018, p. 3)

Há outras cifras semelhantes à ROT-13. Cada uma delas se encarrega de realizar algum tipo de codificação especifica com relação aos caracteres usados para elaborar uma mensagem. Por exemplo, a cifra ROT-5 se ocupa em codificar os algarismos da base decimal 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. A cifra ROT-13 que mencionamos anteriormente codifica somente nosso alfabeto usual. Para codificarmos, tanto letras quanto números, utilizamos uma junção das cifras ROT-13 e ROT-5 para obtermos a chamada cifra ROT-18. Todas elas foram desenvolvidas para fins elementares de criptografia básica (cuja ação não vai além de codificações de informações com importância inferior as informações militares ou governamentais). Não representando, portanto, um método criptográfico seguro[12].

Nas subseções que seguem, voltaremos a falar sobre a cifra de César e suas ramificações, destacando como tal cifra poderia ser melhorada e qual a sua fraqueza em termos de segurança. Na oportunidade destacaremos outras cifras igualmente importantes, porém, com características diferentes das cifras que vimos até o momento. Nossa intenção será tratar o nascimento da criptoanálise e quais foram as primeiras cifras desenvolvidas como alternativa para vencer uma nova técnica de decodificação de mensagem que foi desenvolvida no oriente e causou enormes transtornos para os criptógrafos que utilizavam cifras de substituição semelhantes as que apresentamos anteriormente. Abordaremos novamente o conceito de cifra, porém agora relacionando com o conceito de código.

2.1.4 Cifras e Códigos: qual a diferença?

Primeiramente, é preciso deixar claro que, estritamente falando, cifra e código não é a mesma coisa, embora em alguns momentos estas ideias se confundam. O conceito de cifra já foi mencionado na Página 32 e se refere a qualquer mecanismo de criptografia que se resuma a converter cada letra do alfabeto original em outra letra ou um símbolo qualquer. Já vimos alguns exemplos de cifras nas seções precedentes. Quando usamos uma cifra para modificar o significado real de uma mensagem, dizemos que a mensagem foi *cifrada*. Porém, utilizaremos, como já vínhamos fazendo, a palavra codificar para denotar o processo de mudar o significado original de uma mensagem por meio de um método de criptografia, seja

[12] Veja mais: <http://www.webutils.pl/ROTencode>. Acesso em: 27 out. 2019.

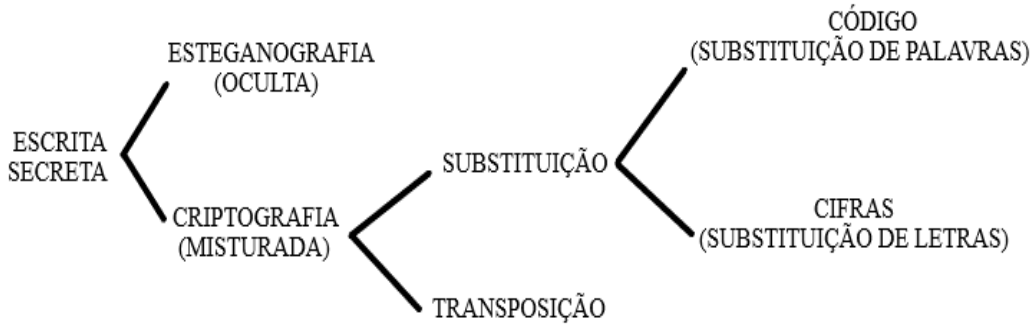
ele cifra ou não. Então, decodificar será usado para descrever o processo inverso. Já a palavra *decifrar* é, precisamente falando, o processo de desfazer uma codificação que foi feita através de uma cifra (SINGH, 2004). Entretanto, há autores como Sautoy (2007) que entende este conceito como sendo o ato de um indivíduo descobrir o texto original de uma mensagem por meio do texto codificado, sendo que para isso ele não utiliza o processo específico de decodificação. Ou seja, decifrar para Sautoy (2007) é quebrar o procedimento de codificação, descobrir a mensagem verdadeira, sem, no entanto, ser o legítimo destinatário daquela mensagem. É com este entendimento que optamos em usar a palavra decifrar com este significado.

Por outro lado, "a palavra código se refere a um tipo especial de comunicação secreta, cujo uso vem declinando ao longo dos séculos" (SINGH, 2004, p. 14). Um código é um método de criptografia mais geral do que as cifras no sentido de que agora palavras ou até mesmo frases inteiras podem ser substituídas por outras palavras, números ou símbolos quaisquer. É como se os códigos fossem uma generalização das cifras. Por exemplo,

> [...] os agentes secretos usam nomes em códigos no lugar de seus nomes verdadeiros, de modo a esconder suas identidades. De modo semelhante, a frase "ataque ao amanhecer" pode ser substituída pela palavra código "júpiter" e esta palavra será transmitida ao comandante, no campo de batalha, com o fim de confundir o inimigo. (SINGH, 2004, p. 14)

Ou seja, o envio de mensagens por meio de códigos se caracteriza pela definição dos símbolos ou palavras-códigos que substituirão o conteúdo da mensagem original. Neste caso, o código age como um simplificador da mensagem em questão, pois um trecho ou até mesmo a própria mensagem inteira, podem ser substituídos por um único símbolo ou uma palavra. Este tipo de característica não é comum às cifras. Cabe, então, uma pergunta: qual a diferença entre código e cifra? "tecnicamente um código é definido como uma substituição de palavras ou frases, enquanto a cifra é definida como uma substituição de letras" (SINGH, 2004, p.47). Porém, haverá ocasiões em que vamos nos referir a um tipo de método criptográfico como sendo código, mesmo ele não sendo, necessariamente, um, segundo a definição anterior. Ficará claro no contexto se estamos tratando de uma cifra ou código. No esquema abaixo apresentamos uma divisão das ramificações da escrita secreta até agora apresentadas neste trabalho.

Figura 6 – Algumas Ramificações da Escrita Secreta



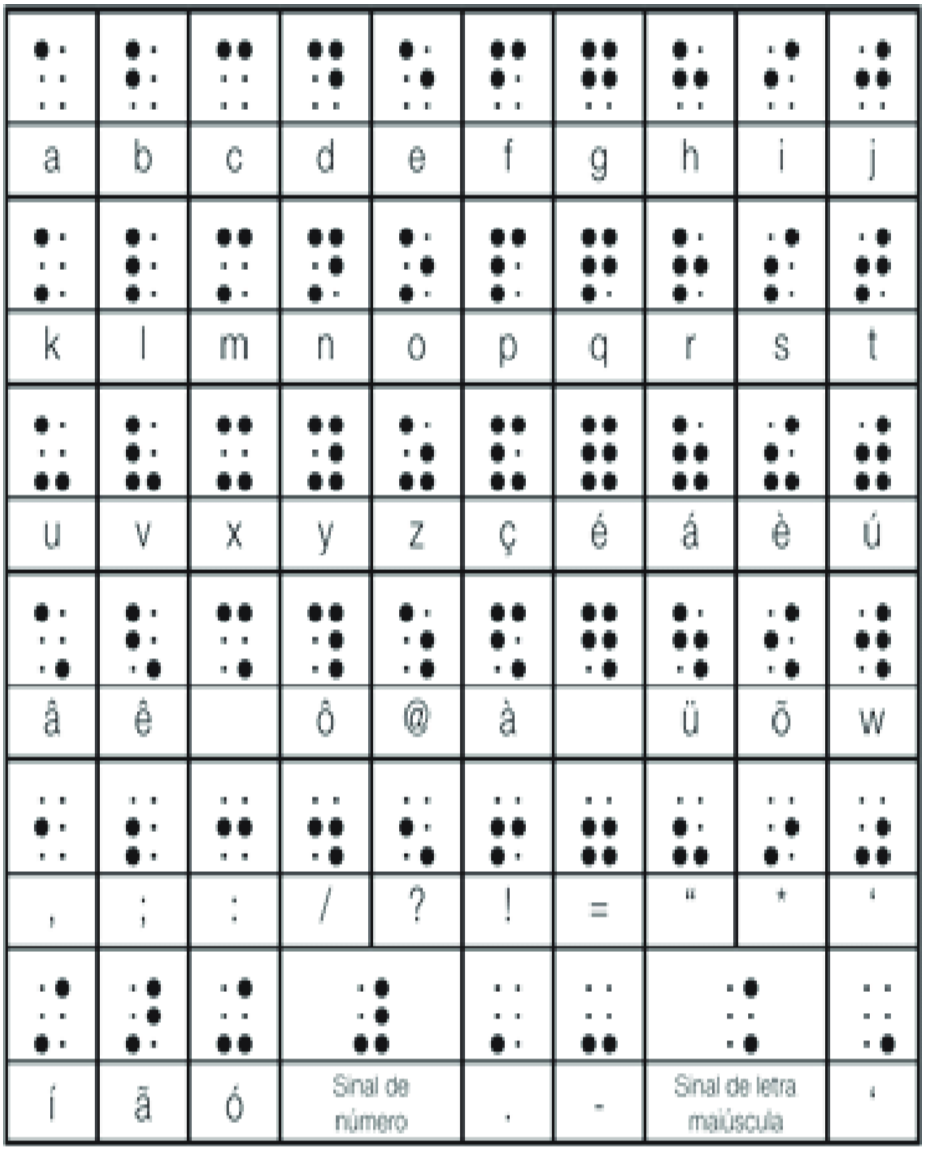
Fonte: Singh (2004). Acesso em: 24 out. 2019

Dentre inúmeros códigos desenvolvidos ao longo da história da criptografia, destacaremos dois por se tratarem de sistemas revolucionários que contribuíram fortemente para o desenvolvimento das comunicações e são, até hoje, mundialmente usados: o *Código Braille* e o *Código Morse*. O código Braille (ou sistema Braille) foi desenvolvido por Louis Braille (1809 - 1852), um francês que ficou completamente cego ainda criança em decorrência de um acidente sofrido quando manipulava as ferramentas da oficina de seu pai (COSTA, 2009). Uma ligeira versão do sistema criado por Braille foi proposto inicialmente por Charles Barbier de la Serre, um capitão de artilharia que desenvolveu um tipo de código para se comunicar com seus soldados. Daí, poderíamos dizer que o código Braille teve sua essência em um método de esteganografia militar[13]. A ideia do código de Barbier era que os soldados pudessem ler mensagens no escuro (por isso o código ficou conhecido como *escrita no escuro*) e, para isso, as mensagens eram transmitidas por meio de pontos em alto relevo que poderiam ser "lidas" com as pontas dos dedos. Já a versão de Braille ainda conserva a disposição de pontos em alto relevo, porém é mais completa e menos complexa, "é constituído por 63 sinais formados por pontos a partir do conjunto matricial ⁝⁝ (123456). Este conjunto de 6 pontos chama-se, por isso, *sinal fundamental*" (BRASIL, 2006, p.17). Denominamos *Célula Braille* a qualquer disposição dos pontos do conjunto fundamental, isto é, a qualquer configuração que gere um sinal produzido nesse sistema. A célula vazia é aquela

[13] Não seria correto afirmar que o código desenvolvido por Barbier era um método criptográfico, pois sua intenção não era modificar o conteúdo da mensagem de modo que só o receptor pudesse entender, e sim desenvolver algum procedimento para esconder a mensagem através de símbolos de modo que os soldados pudessem ler no escuro. Isto está mais próximo de um método de esteganografia. Da mesma forma, não seria aconselhável dizer que os códigos Braille e Morse são métodos criptográficos. Eles não desempenham tal função, mas são meios de transmitir uma mensagem por meio de símbolos. Em suma, vamos chamá-los apenas de códigos.

que nenhum ponto se destaca em relação aos demais. Ela também é considerada um símbolo. Logo, o código Braille passa a ser formado por 64 símbolos. A Tabela 2 ilustra a codificação feita via Braille para o alfabeto comum e mais alguns símbolos.

Tabela 2 – Alfabeto Braille e Outros Símbolos



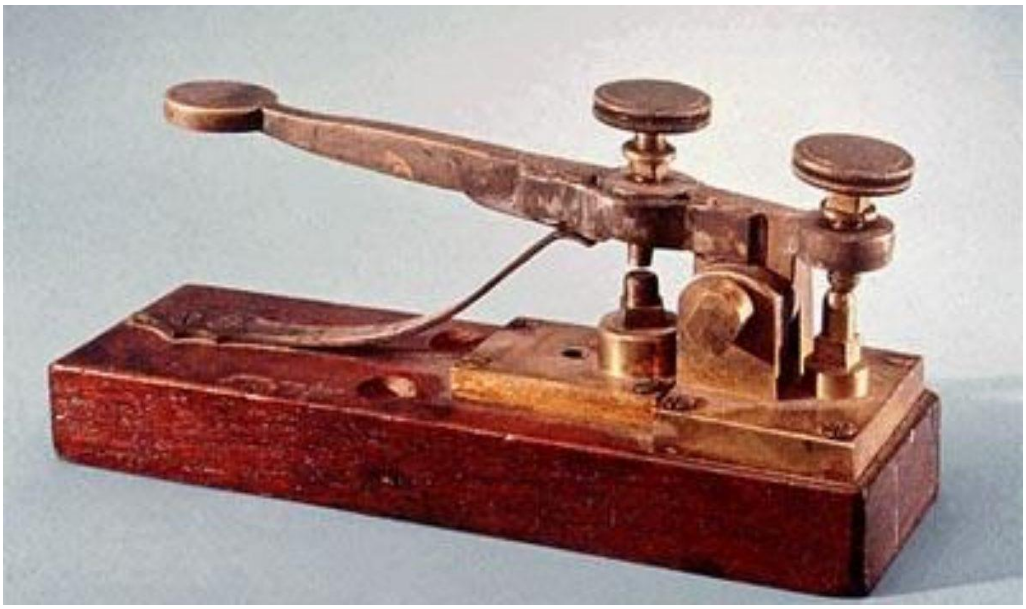
Fonte: <https://images.app.goo.gl/e413h53xenzkDhBX8>. Acesso em: 19 Out. 2019

O sistema Braille foi introduzido no Brasil em 1854 na inauguração do Instituto Benjamin Constant (conhecido como Imperial Instituto dos Meninos Cegos), no Rio de Janeiro (COSTA, 2009). Hoje, universalmente usado, o código Braille é uma das ferramentas

mais importantes para que pessoas com deficiências visuais possam ter acesso ao conhecimento por meio da leitura e escrita.

Com relação ao código Morse, o mesmo teve como inventor Samuel Finley Breese Morse (1791 - 1872)[14] em 1835, com o auxílio de Joseph Henry (1797 - 1878)[15] e Alfred Vail (1807 - 1859)[16]. Em 1835, Morse criou um aparelho que servia para enviar mensagens à longa distância por meio da rede elétrica. Este aparelho ficou conhecido como *telégrafo elétrico*. O telégrafo foi planejado para mandar e receber mensagens por meio de pulsos elétricos produzidos através de um eletroímã que era controlado pela corrente elétrica.

Figura 7 – O telégrafo



Fonte: <https://images.app.goo.gl/2uRBPGftafCZU3448>. Acesso em: 28 out. 2019

O código desenvolvido por Morse para mandar mensagens através do telégrafo se baseava exatamente nessa característica de envio por meio de pulsos elétricos.

[14] Foi inventor, físico e pintor estadunidense. Fonte: < https://pt.wikipedia.org/wiki/Samuel_Morse>. Acesso em: 28 out. 2019
[15] Cientista estadunidense. Fonte: < https://pt.wikipedia.org/wiki/Joseph_Henry>. Acesso em: 28 out. 2019
[16] Maquinista e inventor estadunidense. Fonte: < https://pt.wikipedia.org/wiki/Alfred_Vail>. Acesso em: 28 out. 2019

> [...] o sistema telegráfico dos três americanos, inaugurado em 1844, foi projetado para fazer registros em uma fita de papel quando correntes elétricas fossem recebidas. O receptor original do telégrafo Morse utilizava um mecanismo de rodas mecânicas para mover a fita. Quando uma corrente elétrica era recebida, um eletroímã acionava uma caneta na fita de papel, que estaria em movimento, fazendo um recorte (**risco**) na fita. Quando a corrente era interrompida, a caneta era retraída, para que a porção da fita que não tivesse sido utilizada continuasse sem marcas. (PORTO, [entre 2006 e 2019], p.1, grifo nosso)

Este risco e a parte não tocada pela caneta passaram a ser caracterizados como “traço” (-) e “ponto” (.). Assim, através do código criado por Morse as mensagens poderiam ser codificadas através desse sistema de ponto e traço como sinais a serem decodificados pelo receptor. “Originalmente, Morse imaginou numerar todas as palavras e em transmitir seus números através do telegráfo. O receptor, usando um enorme ‘dicionário’ decifraria a mensagem onde as letras do alfabeto foram definidas pelo padrão ‘ponto e traço’ citado anteriormente” (FRANÇA, 2014, p.31, grifo nosso). Coube a Alfred Vail aprimorar o código de Morse, atribuindo um sistema de letras e caracteres especiais de modo a simplificar o código e torná-lo mais completo. Segundo França (2014, p. 31), “este novo código reconhecia quatro estados: voltagem-ligada longa (traço), voltagem-ligada curta (ponto), voltagem-desligada longa (espaços entre caracteres e palavras) e voltagem-desligada curta (espaços entre pontos e traços)”. Vail procurou representar cada letra do alfabeto e outros caracteres por meio de sequências de pontos e traços. Cada letra, número, sinais de pontuação, entre outros símbolos, possuíam sua sequência bem definida de pontos e traços. As letras mais frequentes do alfabeto inglês (alfabeto em questão na época) ficaram com as sequências mais curtas e as letras menos frequentes com as sequências mais longas de pontos e traços, respectivamente, como uma alternativa para deixar o código mais leve, simples e de mais fácil memorização. A Tabela 3 apresenta o alfabeto usual codificado por código Morse, além dos algarismos de 0 à 10 e alguns sinais de pontuação.

Tabela 3 – Alfabeto em Morse e outros caracteres

Letra	Sinal	Letra	Sinal	Número	Sinal	Pontuação	Sinal
a	•—	r	•—•	1	•————	Ponto	••••••
b	—•••	s	•••	2	••———	Ponto e vírgula	—•—•—•
c	—•—•	t	—	3	•••——	Vírgula	•—•—•—
d	—••	u	••—	4	••••—	Dois pontos	———•••
e	•	v	•••—	5	•••••	Interrogação	••——••
f	••—•	x	—••—	6	—••••	Exclamação	——••——
g	——•	y	—•——	7	——•••	Apóstrofe	•————•
h	••••	z	——••	8	———••	Traço de união	—••••—
i	••	ch	————	9	————•	Aspas	•—••—•
j	•———	w	•——	0	—————	Parêntesis	—•——•—
k	—•—	ä	•—•—			Alínea	•—•—••
l	•—••	é/ë	••—••			Sublinhado	••——•—
m	——	ï	—••——			Duplo traço (=)	—••••—
n	—•	ñ	——•——				
o	———	ö	———•				
p	•——•	ü	••——				
q	——•—						

Fonte: <https://images.app.goo.gl/s4nvZb2UoVUzTBJL7>. Acesso em: 29 out. 2019

O código Morse foi rapidamente aceito pela comunidade científica da época, tornando o principal meio de comunicação à distância através de mensagens enviadas pelo telégrafo. As companhias telegráficas eram as responsáveis por coordenar os envios de mensagens (e a cobrar por isso). O código Morse foi muito usado na aviação, nas navegações e no meio militar em guerras. Seu ápice de uso ocorreu no século XIX, sendo utilizados por quase todos os países da Europa, obtendo uma nova versão mais desenvolvida (que ficou conhecida como *código Morse internacional*) em 1865, regulamentada pelo Congresso Internacional Telegráfico (FRANCISCO, 2019). Certamente um dos códigos mais importantes já

inventados. Foi essencial para o desenvolvimento das comunicações à longa distância e proporcionou o início da era da comunicação telefônica.

2.1.5 Análise de frequências e o nascimento da Criptoanálise

Se há a necessidade de proteger informações preciosas enviadas via mensagens, então é porque se pressupõe que essa informação também pode ser do interesse de outras pessoas que não têm autorização para conhecê-la, os intrusos. Neste caso, esses intrusos tentam a todo custo se apossar dessas mensagens procurando entendê-la de alguma forma. Ora, para manter a segurança e sigilo no envio, essas mensagens foram codificadas por métodos de criptografia. Logo, só o emissor e o receptor têm condições de decodificar a mensagem e conhecer seu conteúdo original. Portanto, para o intruso, caso ele consiga interceptar o envio e pôr as mãos na mensagem, o único modo de conseguir conhecer seu conteúdo é "quebrar" o método ou código usado para codificá-la. Esse problema no envio de mensagens fez com que, paralelamente ao desenvolvimento da criptografia, outra ciência igualmente importante se desenvolvesse. Esta ciência é conhecida como *Criptoanálise*. A criptoanálise "permite decifrar uma mensagem sem conhecer a chave. Enquanto o criptográfo desenvolve novos métodos de escrita secreta, é o criptoanalista que luta para encontrar fraquezas nesses métodos, de modo a quebrar a mensagem secreta" (SINGH, 2004, p. 32).

O intruso que citamos anteriormente passará a ser chamado de criptoanalista. Seu principal objetivo é decifrar a mensagem. E decifrar, segundo nossa concepção já mencionada, significa procurar reverter o processo de codificação sem ser o real destinatário da mensagem. As ferramentas que o criptoanalista usa para achar fraquezas nos métodos criptográficos e decifrar as mensagens fazem parte dos *ataques* a estes códigos. Esses ataques são diversos. Uma breve descrição de alguns deles pode ser encontrada em Terada (2000).

A invenção da criptoanálise é devida aos árabes que, além de um grande domínio sobre as cifras de substituição monoalfabéticas, foram os responsáveis por descobrir um meio de decifrar uma mensagem codificada por tais cifras. Porém, antes disso, foi preciso um grande desenvolvimento no conhecimento de algumas ciências, tais como matemática (com ênfase em estatística) e linguística. Além dessa evolução, houve um avanço significativo relacionado aos estudos religiosos (SINGH, 2004).

> Além de uma compreensão maior de assuntos leigos, a invenção da criptoanálise também dependia do crescimento dos estudos religiosos. Grandes escolas de teologia foram fundadas em Basra, Kufa e Bagdá, onde os teólogos examinavam cuidadosamente as revelações de Maomé contidas no **Corão**[17]. Os teólogos estavam interessados em estabelecer a cronologia das revelações, e o faziam contando a frequência das palavras contidas em cada revelação. (SINGH, 2004, p. 33, grifo nosso)

Essa é a essência da criptoanálise: contar a frequência das palavras que aparecem em um texto. Esta atividade evoluiu para a contagem da frequência das letras que compõe um texto. Os estudiosos árabes descobriram que determinadas letras aparecem com mais regularidades, mais frequência, do que outras. Por exemplo, "as letras a e l são mais comuns no idioma árabe, parcialmente devido ao artigo indefinido al-, enquanto a letra j aparece com frequência dez vezes menor" (SINGH, 2004, p. 33).

O fato de que certas letras aparecem com mais frequência do que outras em textos de uma determinada língua foi o grande responsável pelo primeiro avanço significativo da criptoanálise desenvolvida pelos árabes. Apesar de não se saber exatamente quem foi a primeira pessoa a utilizar a frequência das letras como uma técnica de criptoanálise e nem quando isso ocorreu, Singh (2004) assegura que uma das descrições mais antigas dessa técnica aparece em uma obra de um cientista árabe do século IX chamado Abu Yusef. A seguir, apresentamos a descrição feita por Abu Yusef sobre o método de análise de frequências. Esta descrição pode ser encontrada em Singh (2004, p. 33).

> *"Um meio de se decifrar uma mensagem codificada, quando conhecemos seu idioma, é encontrar um texto diferente, na mesma língua, suficientemente longo para preencher uma página. Então contamos a frequência com que cada letra aparece. A letra que aparecer com maior frequência chamamos de "primeira", enquanto a segunda mais frequente recebe o nome de "segunda", a terceira em ordem de frequência vira "terceira" e assim por diante, até contarmos todas as letras diferentes no texto".*
>
> *"Em seguida examinamos o criptograma que desejamos decifrar e também classificamos os seus símbolos. Descobrimos qual o símbolo que aparece com maior frequência e o transformamos na "primeira"*

[17] Ver: <https://www.trt.net.tr/portuguese/programas/2016/03/30/o-corao-o-livro-sagrado-dos-muculmanos-461197>.

> *letra do texto que usamos como amostra. O segundo símbolo mais comum é transformado na "segunda" letra, enquanto o terceiro símbolo mais frequente vira a "terceira" letra e assim por diante, até convertermos todos os símbolos do criptograma que desejamos decifrar".*

O método acima descrito é o que hoje conhecemos como análise de frequências. O que o torna eficaz como método de criptoanálise é o fato de que além de existir letras de uma determinada língua, mais frequentes do que outras, estas frequências são quase que constantes. Isto é, ao estudarmos vários textos em português, por exemplo, veremos que as letras aparecem numa regularidade que, em média, é fixa. Este fato, somado ao método de análise de frequências, possibilita que possamos estudar um texto cifrado, contar a frequência de cada caractere deste texto, e então fazer algumas estimativas estatísticas a fim de determinar quais são os símbolos que estão substituindo cada letra do alfabeto original. Por exemplo, segundo Terada (2000), após análise de vários textos em português, conclui-se que a vogal mais frequente é o *a*, que aparece com uma frequência de 13,5% em média. Ainda segundo Terada, as vogais *e*, *i*, *o* e *u* apresentam as seguintes frequências, respectivamente: 12,5%, 6,0%, 5,5% e 4,5%. Portanto, se num texto cifrado observarmos que uma letra, digamos y, aparece com uma frequência mais ou menos igual a 13,5%, então é muito provável que ela esteja substituindo o *a* no texto original. Da mesma forma pensamos os demais símbolos. É lógico que não há como garantir que o y está substituindo o *a* com 100% de certeza, pois trata-se de uma média, que será melhorada se os textos cifrados forem cada vez maiores[18]. Dependendo da quantidade de texto analisado, estes percentuais podem variar bastante. Usando este pensamento para todas as letras do texto cifrado, podemos desenvolver uma análise que poderá nos dar pistas de como foi realizada a codificação do texto original[19].

A análise de frequência é a principal técnica usada contra as cifras de substituição monoalfabéticas, pois tais cifras possibilitam que as frequências das letras sejam preservadas ao passar para o texto cifrado. Por isso, a análise de frequências é classificada como um ataque estatístico somente ao texto cifrado (TERADA, 2000). A invenção da criptoanálise, em especial da análise de frequências, tornou as cifras de substituição monoalfabéticas frágeis e

[18] O leitor pode consultar a obra Singh (2004) para obter mais informações a respeito do método de análise de frequência aplicado na decifragem de mensagens, inclusive um exemplo prático de como isso pode ser feito.
[19] Este método não é eficiente para textos curtos. Textos longos são mais receptíveis a uma análise bem sucedida.

inseguras. Mas isso teve sua parcela de importância no desenvolvimento da criptografia, pois motivou o desenvolvimento de novas técnicas, mais eficientes, de codificação.

2.1.6 Chaves

Um dos conceitos mais importantes da criptografia é o de *chave*. Para entender o que significa uma chave e qual o seu papel nos métodos criptográficos devemos ter bem claro em mente a diferença entre o método geral de criptografia em uso (que mais adiante vamos chamá-lo de algoritmo) e o procedimento específico de codificação de uma mensagem por meio desse método. Vamos esclarecer isso através de exemplos: Digamos que queremos estabelecer uma comunicação por mensagens e escolhemos uma cifra de César como método de codificação. Ora, de acordo com a definição da cifra de César, qualquer translação do alfabeto entre 1 e 25 letras nos fornece uma maneira de definirmos o alfabeto cifrado. Por exemplo, se deslocarmos o alfabeto uma, duas, três ou quatro letras à frente, obtemos cifras de César cujos alfabetos cifrados são, respectivamente, os seguintes:

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

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

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

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

Assim sendo, cada um desses alfabetos cifrados distintos nos dá uma maneira específica de codificar uma mensagem. Portanto, dizemos que cada um desses alfabetos cifrados constitui uma *chave* para a cifra de César, sendo esta cifra o método geral de codificação. Como há 25 maneiras de transladarmos o alfabeto, então a cifra de César possui 25 chaves.

Mais geralmente, poderíamos pensar em outra cifra de substituição com base na cifra de César, impondo que o alfabeto cifrado seja qualquer permutação do alfabeto original, e não apenas uma translação como mostrado anteriormente. “Neste caso, o algoritmo consiste em substituir cada letra do alfabeto original por uma letra do alfabeto cifrado, e o alfabeto cifrado pode consistir em qualquer rearranjo do alfabeto original. A chave define o alfabeto cifrado exato que será usado em uma codificação em particular” (SINGH, 2004, p. 27).

A importância das chaves está ligada a segurança dos métodos criptográficos. São elas que bem caracterizam a segurança das cifras de substituição, com maior ênfase nos métodos que funcionam com chave única. A quantidade de chaves é que define o grau de segurança dessas cifras no sentido de que se a cifra possui um número muito grande de chaves, então é muito difícil para um intruso quebrá-la por meio de uma tentativa de descobrir a chave certa de codificação. Por exemplo, a cifra de César só possui 25 chaves, então fica fácil para um inimigo tentar descobrir a chave certa por tentativas. Por outro lado, usando a cifra que mencionamos anteriormente, onde o alfabeto cifrado pode ser qualquer permutação das 26 letras do alfabeto original, o número de chaves cresce para 26! (26 fatorial), que é um número gigantesco. Logo, fica praticamente impossível para uma pessoa não autorizada descobrir a chave exata com tantas possibilidades a testar, mesmo que ela saiba qual foi o método utilizado.

O conhecimento do método geral usado para codificar a mensagem pode (ou não) ser do conhecimento do intruso. No entanto, mesmo de posse da cifra em uso, se o mesmo não conhece a chave ou não tem nenhuma condição de obtê-la por qualquer de seus métodos, a mensagem continua em segurança.

> De um modo geral, se um inimigo intercepta uma mensagem em código, ele pode suspeitar qual seja o algoritmo, mas espera-se que ele não conheça a chave exata. Por exemplo, ele pode suspeitar de que cada letra no texto original foi substituída por uma letra diferente, de um alfabeto cifrado, mas é improvável que o inimigo saiba qual alfabeto cifrado foi usado. (SINGH, 2004, p. 27)

Mais importante do que se ter um número imenso de chaves, é saber guardar bem elas, isto é, deve-se manter sempre em segredo a chave, sendo de posse restrita do emissor e receptor. A justificativa para isso é óbvia, uma vez que se a chave exata cair nas mãos do inimigo, ele poderá decodificar todas as mensagens que foram codificadas usando aquela chave. Daí a relevância do sigilo da chave, que supera o sigilo do algoritmo utilizado. Ou seja, o conhecimento do algoritmo de criptografia utilizado não é mais importante do que manter em segredo a chave. Segundo Singh (2004, p. 28),

> 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 Cryptographie 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, 2004, p. 28)

Criptossistemas estão intimamente relacionados ao conceito de *função*, generalizam e conceituam precisamente a ideia de métodos criptográficos, e serão abordados no Capítulo 4. Já criptoalgoritmo é um novo nome usado para se referir a algoritmos de criptografia. É preciso ressaltar que essa preocupação em manter em sigilo a chave de codificação só se faz presente na criptografia de chave privada (que abordaremos mais adiante). Como até agora nosso métodos estão nessa classe de criptografia, a discussão acima é relevante e mostra a importância do sigilo da chave nesse ambiente. No entanto, existe outro tipo de criptografia, que atua com duas chaves, onde a chave de codificação pode ser conhecida por qualquer um, mas a chave de decodificação é mantida em segredo. Faremos uma breve apresentação desses tipos de criptografia na Seção 2.2.

2.1.7 Cifras de substituição Monoalfabéticas e Polialfabéticas

A cifra de César e as demais cifras de substituição que já conhecemos até o momento possuem uma característica comum no que tange seu modo de agir: cada uma delas faz com que cada letra do alfabeto original seja substituída por uma única letra do alfabeto cifrado. Quando isso acontece, dizemos que a cifra usada é *monoalfabética*. Mais geralmente, "uma cifra monoalfabética é construída ao fazer corresponder cada letra distinta do alfabeto a exatamente um símbolo distinto" (FRANÇA, 2014, p.19). Ainda segundo França (2014), ao se considerar um conjunto de símbolos que serão usados para substituir os *caracteres* de um texto legível e se esta substituição ainda preserva a característica de trocar cada caractere do texto original por um único símbolo substituto, então a cifra ainda é considerada monoalfabética.

Da mesma forma, se em uma cifra de substituição pode-se trocar cada caractere do texto original por dois ou mais símbolos do alfabeto cifrado, diremos que a mesma é uma cifra de substituição *polialfabética.* Se denominarmos por alfabeto cifrante o conjunto de símbolos (letras e outros caracteres) que serão usados para substituir as letras da mensagem original, então denominaremos de cifra polialfabética toda aquela que admitir mais de um alfabeto cifrante (FRANÇA, 2014). É possível, em uma cifra de substituição polialfabética, utilizar vários alfabetos cifrantes para codificar as letras de uma mesma mensagem.

Em razão da fragilidade das cifras de substituição monoalfabéticas frente à análise de frequências, as cifras de substituição polialfabéticas surgiram como uma brilhante solução

para vencer este tipo de criptoanálise. Este tipo de cifra é imune à análise de frequência por se utilizar vários alfabetos cifrados para codificar o texto de uma mesma mensagem. Isso dificulta a contagem das frequências das letras que aparecem na mensagem cifrada.

Um dos primeiros exemplos de cifras de substituição polialfabética foi proposto por Leon Battista Alberti (1404 - 1472) no século XV.

> Naquela época todas as cifras de substituição exigiam um único alfabeto cifrado para codificar cada mensagem. Alberti propôs o uso de dois ou mais alfabetos cifrados, usados alternadamente, de modo a confundir os criptoanalistas em potencial. (SINGH, 2004, p.64)

Isso significa que cada letra que aparece na mensagem original poderá ser substituída de duas maneiras diferentes na mensagem codificada. Ou seja, podemos alternar os alfabetos cifrados para codificar uma mensagem. Na Tabela 4, ilustramos um exemplo da cifra proposta por Alberti. Esta tabela pode ser encontrada em Singh (2004).

Tabela 4 – Cifra de Alberti

Alfabeto original:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabeto cifrado 1:	F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
Alfabeto cifrado 2:	G O X B F W T H Q I L A P Z J D E S V Y C R K U H N

Fonte: Singh (2004)

De acordo com a tabela anterior, a letra **a** pode ser substituída pela letra F ou pela letra G. Da mesma forma, a letra **d** pode ser trocada por V ou por B e assim por diante. Então, se quisermos codificar a palavra *tese,* por exemplo, poderemos substituir o **t** por G, por meio do alfabeto cifrado 1. O **e** pode ser substituído por K ou F. Escolhamos K. A letra **s** passará a ser V, utilizando o alfabeto cifrado 2. A última letra **e** será substituída por F. A palavra tese, codificada, fica assim: GKVF. Veja que a mesma letra **e** foi codificada de duas maneiras distintas. "A vantagem crucial do sistema de Alberti é que a mesma letra do texto original não aparece necessariamente como uma única letra no texto cifrado [...]" (SINGH, 2004, p.64).

No entanto, “embora houvesse descoberto o avanço mais significativo das cifras num período de mil anos, Alberti não conseguiu desenvolver sua ideia, transformando-a num sistema completo de cifragem” (SINGH, 2004, p.64). Coube, então, a um trio de intelectuais a tarefa de dar continuidade ao trabalho de Alberti e desenvolver seu trabalho por completo. Johannes Trithemius[20] (1462 - 1516), Giovanni Porta[21] (1535 - 1615) e Blaise de Vigenère[22] (1523 - 1596) deram suas contribuições para que a cifra de Alberti pudesse ser aperfeiçoada. Entretanto, coube a este último, Blaise de Vigenère, dar a versão final da cifra de Alberti. A novidade colocada por Vigenère é que, no lugar de dois, ele utiliza 26 alfabetos cifrados. Cada um desses alfabetos cifrados é do tipo dos da cifra de César, transladado 1, 2, 3,..., 26 letras, respectivamente. Então, cada letra da mensagem original poderá ser codificada de acordo com um desses 26 alfabetos cifrados. Para codificar uma mensagem, usa-se o *quadrado de Vigenère*, (ver Figura 8) que consiste na disposição do alfabeto original (na parte superior) juntamente com os 26 alfabetos transladados. É com ele que podemos nos orientar para seguir os passos corretos de codificação de cada letra do texto a ser codificado.

[20] Pseudônimo de Johann Heidenberg, polímata e monge beneditino alemão. Foi lexicógrafo, cronista, criptógrafo e ocultista. Dentre suas obras há uma que trata da esteganografia, denominada *steganographia*, escrita por volta de 1499. Saiba mais em: <https://www.renaissanceastrology.com/trithemius.html> e <https://pt.wikipedia.org/wiki/Johannes_Trithemius>. Acesso em: 23 out. 2019.

[21] Giovanni Battista Della Porta. Filósofo, Cosmológico e Dramaturgo italiano. Escreveu inúmeros trabalhos sobre os mais variados temas. Dentre eles, destaca-se um sobre criptografia, onde é descrito um dos primeiros exemplos de cifra de substituição polialfabética. Veja mais em: <https://pt.wikipedia.org/wiki/Giovanni_Battista_della_Porta>. Acesso em: 24 out. 2019.

[22] Diplomata e criptógrafo francês. Fonte: <https://en.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re>. Acesso em: 24 out. 2019.

Figura 8 – 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**
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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: <https://images.app.goo.gl/M3AHJ44PtX7KeZie9>. Acesso em: 24 out. 2019.

É claro que existem inúmeras maneiras de se codificar uma mensagem por esse método. Recaímos então naquele problema sobre essa codificação não ser aleatória. Isso causaria sérios problemas para o emissor e o destinatário. Então, para resolver este problema, usa-se uma *palavra-chave* (ou *frase-chave*) como meio de segurança para lembrar os passos da codificação e, por outro lado, efetuar a decodificação. Cada letra da palavra-chave indicará qual foi a linha utilizada no quadrado de Vigenère. Desse modo, suponhamos que a mensagem "*abortar a missão imediatamente*" deva ser codificada por meio da cifra de Vigenère. O emissor e o receptor combinam que a palavra-chave a ser utilizada será "lutar". Então, para codificar a mensagem, o emissor começa escrevendo repetidas vezes a palavra-chave acima ou abaixo da mensagem de modo que cada letra da mensagem esteja em correspondência com uma letra da palavra-chave, como mostra a Tabela 5 a seguir.

Tabela 5 – Utilizando a palavra-chave

Palavra-chave	**l u t a r l u t a r l u t a r l u t a r l u t a r l u**
Mensagem	a b o r t a r a m i s s a o i m e d i a t a m e n t e

Fonte: Autoria própria

Feita esta associação, o emissor passa a codificar cada uma das letras da mensagem. O proceder do emissor será o seguinte: para codificar a primeira letra da mensagem, a letra **a,** ele nota de inicio que a letra que está associada ao **a** é o **l.** Então, como dissemos anteriormente, esta letra **l** indica uma linha do quadrado de Vigenère, que no caso é a 12ª linha. Sendo assim, para achar a letra substituta do **a**, o emissor considera a coluna do quadrado de Vigenère correspondente à letra **a**, que no caso é a 1ª coluna, e observa a letra que está na intersecção dessa coluna com a 12ª linha, que no caso será o próprio **l**. Portanto, a primeira letra da mensagem será substituída pela letra **l.** Da mesma forma, para codificar a segunda letra da mensagem, a letra **b**, o emissor nota que ela está associada à letra **u** na Tabela 3 e que ela determina a 21ª linha do quadrado de Vigenère. Como a letra **b** define a 2ª coluna, a letra que se encontra na intersecção da 2ª coluna com a 21ª linha é o **v**. Logo, a segunda letra da mensagem será substituída pela letra **v**. O emissor repete este procedimento para todas as letras da mensagem, codificando a mensagem por completa por meio da cifra de Vigenère. A Tabela 6 a seguir mostra o resultado final da codificação.

Tabela 6 – Codificando a mensagem

Palavra-chave	**l u t a r l u t a r l u t a r l u t a r l u t a r l u**
Mensagem	a b o r t a r a m i s s a o i m e d i a t a m e n t e
Mensagem codificada	L V H R K L L T M Z D M T O Z X Y W I R E U F E E E Y

Fonte: Autoria própria

A palavra-chave é importante na utilização da cifra de Vigenère porque permite ao emissor e receptor memorizar facilmente a maneira de codificar e decodificar as mensagens trocadas. Sem contar que, uma vez definida essa palavra-chave ou frase-chave, o emissor e o receptor tem total sigilo sobre a mesma, pois podem simplesmente guardar essa palavra ou frase na mente, tornando pouco provável o conhecimento dela por parte de intrusos. Assim sendo, essas palavras ou frases que são usadas como auxiliares para a codificação de mensagens pela cifra de Vigenère constituem, literalmente, chaves dessa cifra, no sentido que abordamos na Seção 2.1.5. Todavia, é fácil notar que há uma quantidade muito grande de chaves para esta cifra, pois qualquer palavra ou frase podem ser usadas como chaves para esse método. Sem contar que existem as maneiras aleatórias de codificação, as quais podem ser descritas por meios de regras estabelecidas ou passos realizados para efetuar a codificação de uma determinada mensagem.

2.1.8 O conceito de Algoritmo

Os métodos gerais de codificação são chamados de *Algoritmos*. O termo algoritmo aparece com muita frequência em criptografia. Não é por menos, já que se constitui de uma noção fundamental nessa ciência (e em geral para a ciência da computação), veja Brookshear (2013). Portanto, precisamos entender a ideia intuitiva de algoritmo. Assim, "informalmente, um algoritmo é um conjunto de passos que define como uma tarefa é realizada" (BROOKSHEAR, 2013, p. 2). Esse conjunto de passos, poderíamos encarar como uma receita para resolver determinada classe de problemas (a tarefa) (COUTINHO, 2005).

Existem muitos algoritmos e lidamos com eles o tempo todo. Por exemplo, uma receita culinária é um exemplo simples de algoritmo. Considere a tarefa de fazer um bolo.

> Um bom livro de receita tem logo depois do nome do bolo, uma lista de ingredientes necessários à sua confecção. Seguem-se as instruções do que fazer com os ingredientes para chegar ao objetivo; coisas como: peneire, misture, bata, asse. Finalmente, temos o resultado: o bolo pronto. (COUTINHO, 2005, p.17)

O funcionamento dos algoritmos imita o processo de fabricação de um bolo. O que chamamos de *Entrada* e *Saída* do algoritmo corresponde, respectivamente, aos ingredientes e ao bolo pronto. O algoritmo é então o conjunto das instruções para fazer o bolo dados os ingredientes. De modo geral, o algoritmo é caracterizado pelo conjunto formado por sua entrada, saída e a receita para a realização do processo.

A matemática é recheada de importantes e fundamentais algoritmos. Vamos tratar alguns desses algoritmos, tais como Algoritmo de Euclides e Algoritmo da divisão, no Capítulo 3. Existem algoritmos de fatoração (Crivo de Eratóstenes, Algoritmo de fatoração de Fermat, algoritmos modernos de fatoração, como Crivo Quadrático, entre outros). Existem algoritmos para testar primaridade (testar se um número inteiro é primo, ou não), para resolver Equações Diofantinas, Congruências Lineares, etc. O leitor interessado no assunto pode consultar Coutinho (2005) e Martinez *et al*. (2013).

Na criptografia o algoritmo é o próprio método criptográfico. Sua entrada é a mensagem original, e sua saída a mensagem codificada. O algoritmo propriamente dito é o passo a passo de como a codificação é realizada.

Se tratando de algoritmos de modo geral, é claro que se desejamos realizar alguma tarefa por meio de um, duas importantes perguntas devem ser feitas: Primeira, dada a entrada do algoritmo, realmente chegaremos a um resultado conveniente? E segunda, este resultado é alcançado em tempo finito (e curto, de preferência)? É sabido que existem processos que podem ser realizados infinitamente, e algoritmos que se baseiam em processos desse tipo não são descartados, veja Brookshear (2013), Capítulos 0 e 5. Entretanto, para os interesses em criptografia, os algoritmos devem se basear em procedimentos que podem ser realizados em tempo finito, caso contrário nunca teríamos a mensagem codificada. Assim, segundo Coutinho (2005), um conjunto de instruções pode ser considerado um algoritmo para resolver determinado problema se for satisfeitas as seguintes condições: (a) essas instruções, ao serem realizadas, devem conduzir a um resultado. (b) o resultado deve ser o esperado. Ou seja, usando uma terminologia mais rigorosa, o algoritmo deve *convergir* para uma solução do problema.

Estas considerações devem bastar para que o conceito de algoritmo seja entendido. No próximo capítulo iremos estudar um importante algoritmo de criptografia, o RSA. Este é, portanto, o principal exemplo de algoritmo criptográfico que iremos abordar. No Capítulo 4 iremos considerar mais alguns algoritmos simples de codificação, mas a importância deles reside no caráter didático, pois os mesmos serão usados como fonte para tratar assuntos de matemática básica.

2.2 Criptografia de Chave Privada e Criptografia de Chave Pública

Nesta seção nosso objetivo é dar uma breve introdução às subdivisões da criptografia, que são as seguintes: Criptografia Simétrica, conhecida como Criptografia de Chave Privada e Criptografia Assimétrica, conhecida também como Criptografia de Chave Pública. Como um tratamento mais detalhado sobre esses ramos da criptografia fogem inteiramente dos objetivos deste trabalho, trataremos apenas de apresentar o significado e as características de cada um deles.

2.2.1 Criptografia de Chave Privada

Ao tratamos de algumas das cifras clássicas em seções anteriores, vimos que as mesmas são métodos criptográficos que utilizam apenas uma chave para desenvolver os processos de codificação e decodificação. Por exemplo, as codificações feitas por métodos de substituição simples podem ser facilmente desfeitas, isto é, a mensagem pode ser decodificada (ou decifrada) se soubermos como ocorreu a substituição, ou seja, qual o alfabeto cifrado. Assim, o conhecimento da chave usada para codificação (o processo específico de codificação) acarreta o conhecimento do processo de decodificação. Afinal, é só reverter o processo. Dizemos nesse caso que a cifra de substituição simples é um método de criptografia de chave privada porque usa apenas uma chave e esta chave, obviamente, deve ser mantida em segredo, sendo de posse restrita do emissor e destinatário legítimos. A área da criptografia que abrange os métodos (algoritmos) criptográficos de chave privada chama-se Criptografia de Chave Privada (ou simétrica).

Existem muitos exemplos de métodos criptográficos de chave privada. Os métodos que vimos até agora são todos de chave privada. Existem outros mais modernos e sofisticados que desempenham papel importante na segurança computacional. Entre eles podemos destacar os seguintes: O Data Encryption Standard (DES), criado pela International Business Machines (IBM) no ano de 1977, considerados um dos melhores algoritmos do mundo, tomado como padrão de criptografia nos Estados Unidos, até perder esse posto para seu sucessor Advanced Encryption Standard (AES). “Em outubro de 2000, o secretário de comércio dos Estados Unidos anunciou o novo Padrão Avançado de Codificação Criptográfica (Advanced Encryption Standard) proposto à nação” (BUCHMANN, 2002). O

International Data Encryption Algorithm (IDEA) é outro algoritmo de chave privada criado no ano de 1991 por James Massey e Xuejia Lai (FRANÇA, 2014).

É fácil perceber qual a fragilidade dos métodos de criptografia de chave privada. Como a mesma só trabalha com uma chave, para se desenvolver uma troca de mensagens o emissor e o destinatário deveriam intercambiar a chave usada antes de realizar a troca de mensagens. Esse intercâmbio, claro, poderia ser feito pessoalmente, caso os envolvidos se encontrassem para trocar as chaves. Ou então eles poderiam enviar a chave por mensagem através de um veículo de comunicação qualquer. Acontece que em ambos os casos a chave não estaria segura e poderia facilmente cair em mãos inimigas. Esta situação se agrava quando a troca de mensagens acontece entre muitos envolvidos. A segurança e gerenciamento dessas chaves torna-se um caos.

Imagine esse tipo de criptografia como segurança hoje na internet. Se desejássemos efetuar uma compra em uma loja virtual qualquer, teríamos que esperar a loja mandar uma mensagem informando como deveríamos codificar os nossos dados pessoais para efetuar o pagamento da nossa compra, isto é, a loja mandava a chave de codificação para que pudéssemos codificar, por exemplo, os dados do cartão de crédito, para pagar a compra. Porém, como a comunicação entre loja e comprador estava sendo realizada por meio da internet, a segurança da chave enviada pela loja poderia ser violada por terceiros e, consequentemente, os nossos dados pessoais não estariam seguros (SAUTOY, 2007).

2.2.2 Criptografia de Chave Pública

Felizmente um novo tipo de criptografia foi proposto em 1976 para acabar com o problema no gerenciamento da chave privada (veja Seção 3.2, Capítulo 3). Esse novo tipo de criptografia traz como novidade o fato de que ele funciona com duas chaves distintas, uma para codificação e outra para decodificação, e o conhecimento da chave de codificação não possibilita decodificar a mensagem. Ou seja, a chave de codificação pode ser pública e só quem poderá decodificar a mensagem é o real destinatário. A chave de codificação é então chamada de chave pública e a chave de decodificação é a chave privada e deve ser mantida em segredo. Sobre o funcionamento deste novo tipo de criptografia, Sautoy (2007, p. 243) acrescenta:

> O sistema de criptografia de chave pública é como uma porta com duas chaves diferentes: a chave A tranca a porta, mas uma chave diferente, B, a destranca. Então, não é mais necessário manter qualquer confidencialidade em relação à chave A. Distribuir cópias dela não compromete a segurança. (SAUTOY, 2007, p. 243)

O primeiro método de criptografia de chave pública desenvolvido foi o RSA. Este método é abordado brevemente neste trabalho no Capítulo 3 como aplicação de noções básicas de aritmética. A criptografia de chave pública propõe o desenvolvimento de um método criptográfico que atue com duas chaves distintas. Neste caso, costuma-se dizer que os métodos de criptografia de chave pública atuam baseados numa função (bijetiva) de mão única (FRANÇA, 2014). Isso quer dizer que esses métodos são baseados em processos que, em essência, são fáceis de ser realizados, mas impossíveis de serem revertidos sem o uso da chave privada. Pense, por exemplo, na porta com duas chaves distintas. É fácil fechar a porta com a chave A, mas impossível abri-la com a mesma chave. O método RSA se baseia num problema dessa natureza, que é o problema da fatoração de números inteiros. Daremos mais esclarecimentos sobre isso no Capítulo 3, mas para o leitor interessado em saber mais sobre a história e desenvolvimento da criptografia de chave pública e o método RSA sugerimos uma consulta às obras Sautoy (2007) e Singh (2004).

3 APLICAÇÕES I: ARITMÉTICA BÁSICA EM CRIPTOGRAFIA RSA

"Os números inteiros desempenham um papel fundamental na criptografia" (BUCHMANN, 2002, p.11). Entretanto, o estudo sobre os métodos clássicos de criptografia que fizemos até agora, baseado nas cifras, ainda não nos ajuda a entender o porquê dos números inteiros serem tão importantes para a segurança da criptografia moderna. Isto se justifica pelo fato de que as cifras clássicas eram métodos de criptografia que tinham sua segurança baseadas em procedimentos que alteravam o alfabeto original, mudando a característica das letras para que pudesse ser realizada a codificação. Quanto mais bem elaborado fosse esse procedimento e maior fosse o número de chaves possíveis, melhor seria a cifra, uma vez que ela seria mais difícil de ser quebrada.

A matemática, nesse estágio da criptografia, ainda não era utilizada no desenvolvimento de técnicas para impor maior segurança aos métodos criptográficos. Daí os números inteiros (positivos) só apareciam em suas funções naturais, expressando quantidades relacionadas com esses métodos. Por exemplo, utilizamos números inteiros positivos e noções a eles relacionadas para contar o número de chaves das cifras de transposição. Foi a partir da criação da criptografia de chave pública, ou assimétrica, que a matemática, em particular a teoria dos números, passou a ocupar um lugar de destaque no mundo dos códigos secretos. A criptografia moderna tem hoje suas bases fixadas em problemas da teoria dos números e é isso que a torna tão segura.

Portanto, com o intuito de apresentar um exemplo de método criptográfico de chave pública e estudar os conceitos de aritmética básica contidos no seu desenvolvimento, o presente capítulo tem por finalidade explorar o *método RSA*, destacando como o mesmo está definido, seu funcionamento e sua segurança. Para isto, como o método RSA se baseia em muitos conceitos elementares de teoria dos números, faremos inicialmente uma revisão sobre esses conceitos, procurando mencionar os resultados e propriedades mais importantes para que possamos desenvolver com mais clareza nossa análise sobre como essas noções estão relacionadas com a criptografia do RSA. É preciso frisar que nosso interesse aqui é investigar a matemática básica presente na criptografia. Sendo assim, uma análise mais profunda sobre criptografia RSA, e mais geralmente sobre criptografia de chave pública, foge inteiramente dos nossos objetivos e, portanto, não será realizada.

Quanto à apresentação de conceitos envolvendo teoria dos números, faremos o possível para simplificar as notações, deixar mais claras as definições e as demonstrações que

aparecerão. Exemplos serão dados para tornar ainda mais fácil a compreensão dos conceitos expostos. É bem verdade que muitos dos conceitos que estudaremos aqui não são tão comuns no currículo de matemática no ensino básico. Mas, nossa abordagem se caracteriza, como na maioria dos livros de teoria elementar dos números (relacionados com criptografia), pelo fato de partirmos de noções simples sobre números inteiros, como divisibilidade e máximo divisor comum, e estendê-las ao ponto que acharmos necessário para o entendimento básico da matemática presente no RSA. Da mesma forma, a abordagem sobre o método RSA será bastante didática, com exemplos que ilustrarão como os processos de codificação e decodificação são realizados, bem como se estrutura a eficiência e segurança desse método. Para o desenvolvimento deste capítulo nos apoiaremos em obras que tratam de teoria dos números ou criptografia. Entre elas, se destacam: Santos (2014), Alencar Filho (1989), Hefez (2014), Shokranian (2005), Terada (2000), Buchmann (2002), Medeiros (2017), Carneiro (2017), Coutinho (2005), entre outros.

3.1 Conceitos básicos de teoria dos números

Como já mencionado, é de fundamental importância o conhecimento dos conceitos básicos de aritmética para melhor compreender a descrição e o funcionamento do método RSA. Mais importante ainda é poder analisar como a matemática básica se faz presente nesse meio. Por isso, nesta seção discutiremos sobre diversos conceitos clássicos da teoria elementar dos números com a intenção de extrair as noções mais importantes e presentes na criptografia RSA, evidenciando como essas noções se fazem presentes na matemática do ensino básico, ou como elas derivam de temas estudados nessa fase de ensino. Números inteiros e suas propriedades, tais como Divisibilidade, Máximo Divisor Comum, Congruências, etc, serão os principais assuntos tratados nesta seção. A seguir, faremos uma breve revisão do conjunto dos números inteiros e do Princípio da Boa Ordenação, com o intuito de fornecer uma breve introdução para os leitores não familiarizados com o tema. Caso contrário, o leitor pode seguir para a Seção 3.2.

3.1.1 Números inteiros e o princípio da boa ordenação

Denomina-se conjunto dos números inteiros, denotado por $\mathbb{Z}$, o conjunto cujos elementos são:

$$\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$$

Ou seja, $\mathbb{Z} = \{\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$. Assim, podemos escrever $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \mathbb{Z}_-$, onde $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ é o conjunto dos números naturais e $\mathbb{Z}_- = \{-1, -2, -3, -4, \ldots\}$ é o conjunto dos números inteiros negativos.

Em $\mathbb{Z}$ estão definidas duas operações[23]: uma adição $(+)$, que a cada par a, b de números inteiros faz corresponder sua soma $a + b \in \mathbb{Z}$, e uma multiplicação (.), que associa a esses inteiros seu produto $a.b \in \mathbb{Z}$. Estas operações possuem as seguintes propriedades:

(i) A adição e a multiplicação são comutativas. Ou seja, para todos $a, b \in \mathbb{Z}$, vale que $a + b = b + a$ e $a \cdot b = b \cdot a$.

(ii) A adição e a multiplicação são associativas. Isto quer dizer que para todos $a, b, c \in \mathbb{Z}$, vale $a + (b + c) = (a + b) + c$ e $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(iii) Existe o elemento neutro da adição, denotado por 0 e chamado de zero. Ou seja, para todo inteiro a, tem-se $a + 0 = 0 + a = a$.

(iv) Existe o elemento neutro da multiplicação, denotado por 1 e chamado de um. Ou seja, para todo inteiro a, vale que $a \cdot 1 = 1 \cdot a = a$.

(v) Para todo $a \in \mathbb{Z}$ existe $-a \in \mathbb{Z}$, tal que, $a + (-a) = (-a) + a = 0$. O elemento $-a$ é chamado de simétrico aditivo de a.

(vi) A multiplicação é distributiva com relação à soma. Ou seja, para todos $a, b, c \in \mathbb{Z}$, vale $a \cdot (b + c) = a \cdot b + a \cdot c$.

(vii) O produto de dois inteiros só é zero se, e somente se, ao menos um dos fatores é zero. Dito de outra forma, isso quer dizer que $a \cdot b = 0 \Leftrightarrow a = 0$ ou $b = 0$.

Além das propriedades de **(i)** a **(vii)**, podemos definir uma relação de ordem $(<)$ em $\mathbb{Z}$ segundo a qual podemos comparar dois números inteiros, como segue.

Definição 3.1 Dados os inteiros a e b, dizemos que a é menor do que b, e indicaremos por $a < b$, quando $b - a \in \mathbb{N}$, isto é, quando $b - a$ for positivo. Analogamente, dizemos que a é

[23] Uma operação num conjunto X nada mais é que uma função (aplicação) $f: X\text{x}X \to X$, que associa a cada par de elementos $x, y \in X\text{x}X$ um elemento $z = f(x, y)$. Veja mais em: Monteiro (1969).

maior do que b, e indicaremos por $a > b$, quando $a - b \in \mathbb{N}$. Quando for verdade que $a < b$ ou $a = b$, diremos que a é menor do que ou igual b e denotaremos por $a \leq b$. Analogamente, $a \geq b$ significa que a é maior do que ou igual b.

Algumas propriedades importantes da relação de ordem (<) em $\mathbb{Z}$ são as seguintes:

a) Como $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \mathbb{Z}_-$, e esses conjuntos são disjuntos, segue que se a é um inteiro não nulo, então ou a é positivo ou a é negativo. Ou seja, se $a \in \mathbb{Z}$ e $a \neq 0$, então $a > 0$ ou $a < 0$.

b) Dados $a, b, c \in \mathbb{Z}$, se for $a < b$ e $b < c$, então $a < c$. (Propriedade transitiva)

c) $a < b$ se, e somente se, $a + c < b + c$, para todos $a, b, c \in \mathbb{Z}$.

d) Sejam $a, b, c \in \mathbb{Z}$, com $c > 0$. Se $a < b$, então $a.c < b.c$. Esta propriedade diz que o sinal da desigualdade não se altera se multiplicarmos o mesmo número positivo em ambos os lados.

e) Sejam $a, b, c \in \mathbb{Z}$, com $c < 0$. Se $a < b$, então $a \cdot c > b \cdot c$. Esta propriedade diz que o sinal da desigualdade é alterado se multiplicarmos o mesmo número negativo em ambos os lados.

Propriedades análogas as anteriores também são válidas se substituirmos $<$ por $\leq$. O leitor interessado pode consultar Monteiro (1969), Hefez (2014) ou Alencar Filho (1989) para obter mais informações a respeito das propriedades da relação de ordem em $\mathbb{Z}$ e suas consequências, bem como outras propriedades derivadas daquelas mencionadas sobre a adição e multiplicação que não citaremos aqui.

A noção de relação de ordem definida em $\mathbb{Z}$ nos possibilita estudar o importante conceito de conjuntos limitados e elemento mínimo de um conjunto de números inteiros, como segue.

Definição 3.2 Um conjunto $A \subset \mathbb{Z}$ é limitado inferiormente quando existe um inteiro a, tal que, $a \leq x$ para todo elemento x de A. Quando esse a pertencer ao conjunto A, diremos que a é o menor elemento (ou elemento mínimo) do conjunto A. Analogamente, $A \subset \mathbb{Z}$ será dito limitado superiormente se existir um inteiro b, tal que, $b \geq x$ para todo $x \in A$. No caso em que esse b pertencer a A, diremos que ele é o maior elemento (ou elemento máximo) do conjunto A. Se A for limitado superior e inferiormente, diremos que A é limitado.

É fácil ver que se o elemento mínimo (resp. máximo) existir, então ele é único.

Um resultado importante que usaremos como técnica de demonstração mais adiante é o chamado *Princípio da Boa Ordenação* (PBO), que assegura que todo subconjunto de $\mathbb{Z}$, não vazio e limitado inferiormente, admite o elemento mínimo. De modo semelhante, pode-se verificar que todo subconjunto de $\mathbb{Z}$, não vazio e limitado superiormente, admite um elemento máximo. O princípio da boa ordenação é inicialmente tratado no conjunto $\mathbb{N}$ dos naturais, onde é assegurado que todo subconjunto não vazio admite um menor elemento. Ele é apresentado como teorema, cuja demonstração é consequência do *princípio de indução finita* (ver, por exemplo, Santos (2014)). Para a demonstração do PBO em $\mathbb{Z}$ podemos usar essa versão em $\mathbb{N}$ para garantir o resultado mencionado anteriormente.

Teorema 3.1 (Princípio da Boa Ordem em $\mathbb{Z}$) Seja $A \subset \mathbb{Z}$, não vazio e limitado inferiormente. Existe $a \in A$, tal que, $a \leq x$ para todo $x \in A$.

Demonstração: A prova deste teorema é bem simples. Primeiro, note que como $A \subset \mathbb{Z}$ é não vazio e limitado inferiormente, então existe $n_0 \in \mathbb{Z}$, tal que, $n_0 \leq x$ para todo $x \in A$. Assim, se for $n_0 \in A$, não há nada o que demonstrar. Por outro lado, se $n_0 < x$, para todo $x \in A$, então $x - n_0 > 0$. Considerando o conjunto S de todos os elementos da forma $x - n_0$, isto é,

$$S = \{x - n_0;\ x \in A\}.$$

Vemos que S é um subconjunto não vazio de $\mathbb{N}$, pois $A \neq \emptyset$. Logo, pelo PBO em $\mathbb{N}$, temos que existe o elemento mínimo de S. Denotemos por p esse elemento mínimo. Daí existe $a \in A$ tal que $p = a - n_0$. Como p é o mínimo de S, então qualquer que seja o $x \in A$, tem-se $p \leq x - n_0 \Longrightarrow a - n_0 \leq x - n_0 \Longrightarrow a \leq x$. Donde concluímos que a é o menor elemento de A. ■

Faremos uso desse princípio na Seção 3.1.3, onde estudaremos o algoritmo da divisão, outra propriedade muito importante do conjunto dos números inteiros.

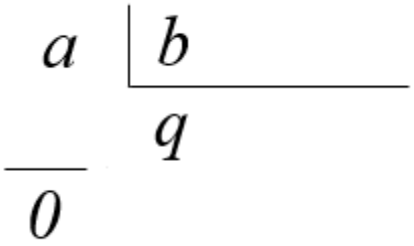
3.1.2 Divisibilidade em $\mathbb{Z}$: definição e algumas propriedades básicas

O conceito de divisibilidade já se faz presente no currículo de matemática do ensino fundamental logo no 6º ano (antiga 5ª série). Lá este conceito é estudado com relação a

números naturais. Aprendemos desde então que dados dois números naturais m e n (com $m > n$, por exemplo), se ao dividirmos m por n e o resto dessa divisão for zero, então m será dito divisível por n, ou que n divide m. Caso o resto seja diferente de zero, m não será divisível por n. Esta definição nos possibilita estudar múltiplos, divisores, números primos, decomposição em fatores primos, máximo divisor comum, mínimo múltiplo comum, entre outros assuntos. Tudo isso tendo como campo de atuação o conjunto $\mathbb{N}$ dos números naturais.

Estendendo a definição dada anteriormente sobre divisibilidade em $\mathbb{N}$ para o conjunto $\mathbb{Z}$ dos números inteiros, obtemos a seguinte versão: dados os números inteiros a e b, com $b \neq 0$, ao dividirmos a por b e o resto for zero, o número a será divisível por b. Caso contrário, a não será divisível por b. No caso em que o resto é zero, podemos escrever $a = b \cdot q + 0$, o que implica $a = b \cdot q$, onde q é chamado de quociente da divisão de a por b (o problema de obter quociente e resto numa divisão será formalizado na próxima seção). Isso é facilmente observado se pensarmos na maneira usual de realizarmos uma divisão. Por exemplo, 60 dividido por 15 dá resto 0 e quociente 4, isto é, $60 = 4 \cdot 15 + 0 = 4 \cdot 15$. Se pensarmos em dois números inteiros genéricos a e b, sendo $b \neq 0$, o esquema a seguir ilustra o caso em que a divisão de a por b dá resto 0.

Figura 9 – Divisão exata de a por b



Fonte: Autoria própria

Da mesma forma, se a e b são inteiros tais que $a = b \cdot q$, com $q \in \mathbb{Z}$, então o resto da divisão de a por b é 0. Com base nessas observações, somos levados à seguinte definição.

Definição 3.3 Sejam dados dois números inteiros a e b, com $b \neq 0$. Dizemos que a é divisível por b, ou que b divide a, quando existe um número inteiro q tal que $a = b \cdot q$.

Observe que $a = b \cdot q$ é o mesmo que $\frac{a}{b} = q$ inteiro. Ou seja, a divisão de a por b é exata. Usamos o símbolo $b|a$ para indicar que b divide a. Quando $b|a$ dizemos também que a é um múltiplo de b, ou que b é um divisor de a. Quando b não divide a usamos a simbologia $b \nmid a$ e isso significa que não existe inteiro q tal que $a = b \cdot q$.

Exemplo 3.1 $2|16$, pois $16 = 2.8$. Já $5 \nmid 12$, pois não existe $q \in \mathbb{Z}$ que verifique a igualdade $12 = 5 \cdot q$.

Observação 3.1 A *relação*[24] b divide a, denotada por $b|a$, recebe o nome de *relação de divisibilidade* em $\mathbb{Z}$ (ALENCAR FILHO, 1989).

A relação de divisibilidade em $\mathbb{Z}$ admite várias propriedades importantes. Além de caracterizar o conjunto dos números inteiros, estas propriedades são usadas constantemente nas demonstrações de resultados que envolvem a noção de divisibilidade. No teorema a seguir iremos destacar algumas dessas propriedades e suas referidas demonstrações. Outras propriedades de importância superior serão desenvolvidas mais adiante.

Teorema 3.2: Sejam a, b e c números inteiros. A relação de divisibilidade admite as seguintes propriedades:

(i) $a|0, 1|a$ e $a|a$. Esta última é chamada de propriedade reflexiva.
(ii) se $a|b$ e $b|c$, então $a|c$. (*propriedade transitiva*)
(iii) se $a|b$, então $a.c|b.c$.
(iv) Se $a|b$ e $b \neq 0$, então $|a| \leq |b|$. Esta propriedade nos ensina que se $a|b$, então, em valor absoluto, a não pode ser maior do que b. Mais ainda, no caso em que temos $a|b$ e for $|a| > |b|$, então se deve ter, necessariamente, $b = 0$.
(v) se $a|b$ e $b|a$, então $|a| = |b|$. Em particular, quando a e b são números naturais, esta propriedade nos garante que se $a|b$ e $b|a$, então $a = b$.
(vi) se $a|b$ e $a|c$, então para todos os números inteiros x e y é válido que $a|(b.x + c.y)$. Ou seja, se a divide b e c ao mesmo tempo, então a divide qualquer combinação linear com coeficientes inteiros de b e c.

[24] Segundo Monteiro (1969), chama-se relação todo subconjunto $\mathcal{R}$ do produto cartesiano EXF, onde E e F são conjuntos. Diz-se nesse caso que $\Re$ é uma relação de E em F. Quando $\Re$ é uma relação de E em E, isto é, num conjunto nele mesmo, dizemos simplesmente que $\Re$ é uma relação sobre E. Assim sendo, podemos dizer que a relação de divisibilidade é uma relação sobre $\mathbb{Z}$. Ou seja, um subconjunto de $\mathbb{Z}x\mathbb{Z}$.

Demonstração:

(i) Segue imediatamente das igualdades: $0 = a \cdot 0$, $a = a \cdot 1$.

(ii) Com efeito, do fato de $a|b$ e $b|c$ segue que existem números inteiros q e r, tais que $b = a \cdot q$ e $c = b \cdot r$. Logo, $c = b \cdot r = (a \cdot q) \cdot r = (q \cdot r) \cdot a$. Como $q \cdot r$ é inteiro, segue que $a|c$.

(iii) Basta notar que se $a|b$, então podemos escrever $b = a \cdot q, q$ inteiro. Logo, $b \cdot c = (a \cdot q) \cdot c = q \cdot (a \cdot c)$. Portanto, $a \cdot c|b \cdot c$.

(iv) De fato, existe q inteiro, tal que, $b = a \cdot q$. Como $b \neq 0$, segue que $q \neq 0$ e $a \neq 0$. Logo, $|q| > 0$, o que acarreta que $|q|$ é um número natural. Assim, temos $|q| \geq 1$. Segue então que: $|b| = |a \cdot q| = |a| \cdot |q| \geq |a| \cdot 1 = |a|$. Portanto, $|b| \geq |a|$.

(v) Basta notar que se $a|b$ e $b|a$, então existem $t, g \in \mathbb{Z}$, tais que $b = a \cdot t$ e $a = b \cdot g$. Logo, $a = b \cdot g = (a \cdot t) \cdot g = a \cdot (t \cdot g)$. Assim, como $a \neq 0$, segue que $t \cdot g = 1$. Isto implica que $|t| = |g| = 1$. Logo, $|a| = |b \cdot g| = |b||g| = |b|$. Onde nesta última igualdade usamos o fato de que $|x \cdot y| = |x| \cdot |y|$ para todos x, y inteiros.

(vi) De fato, basta ver que sendo $a|b$ e $a|c$, então $b = a \cdot q$ e $c = a \cdot r$, onde q e r são números inteiros. Logo, $b \cdot x + c \cdot y = (a \cdot q) \cdot x + (a \cdot r) \cdot y = a \cdot (q \cdot x + r \cdot y)$. Como $(q \cdot x + r \cdot y) \in \mathbb{Z}$, segue que $a|\ (b \cdot x + c \cdot y)$. ■

3.1.3 Divisão Euclidiana

A divisão euclidiana possibilita ampliar a noção de divisão em $\mathbb{Z}$ para os casos em que $b \nmid a$. Ao dividirmos a por b, nem sempre essa divisão será exata, isto é, haverá ocasiões em que o resto será diferente de zero. “No entanto, o conjunto dos números inteiros tem uma característica muito importante que é responsável por várias propriedades nesse conjunto. Em $\mathbb{Z}$ sempre é possível efetuarmos a divisão de dois elementos, obtendo resto pequeno” (MEDEIROS, 2017, p. 31). Este resultado fundamental em teoria dos números é apresentado a seguir como teorema, cuja demonstração se baseia em Alencar Filho (1989) e Hefez (2014).

Teorema 3.3: Sejam a e b dois inteiros dados, com $b \neq 0$. Existem, e são únicos, os inteiros q e r, tais que,

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

Os inteiros q e r com estas propriedades são chamados, respectivamente, de quociente e resto da divisão de a por b.

Demonstração: Como devemos provar a existência e unicidade, faremos a demonstração em duas etapas. Na primeira provaremos a existência de q e r, e na segunda a unicidade dos mesmos. Suporemos também $b > 0$. O caso em que $b < 0$ segue como consequência desse primeiro e será provado por último.

1ª etapa: Consideremos o conjunto S de todos os inteiros não negativos da forma $a - b \cdot x$, com x inteiro. Ou seja,

$$S = \{(a - b \cdot x) \in \mathbb{Z}; a - b \cdot x \geq 0 \text{ e } x \in \mathbb{Z}\}$$

Claramente S é limitado inferiormente (por 0) e não vazio. Com efeito, tomando $x = -|a|$, segue que $a - b \cdot x = a - b \cdot (-|a|) = a + b \cdot |a|$. Como $b > 0$, temos que $b \geq 1$ (já que $b \in \mathbb{Z}$). Segue então que

$$a + b \cdot |a| \geq a + 1 \cdot |a| = a + |a| \geq 0 \Longrightarrow\ a - b \cdot x = a - b \cdot (-|a|) \in S.$$

Portanto, segue pelo princípio da boa ordenação em $\mathbb{Z}$ (Teorema 3.1) que existe o elemento mínimo de S. Seja r esse elemento mínimo. Assim, existirá $q \in \mathbb{Z}$, tal que, $r = a - b \cdot q$. É claro que $r \geq 0$, visto que r é elemento de S.

Note que até agora já temos justificada a existência de inteiros q e r com $r = a - b \cdot q \geq 0$. Para concluir nossa prova de existência será preciso provar que $r < b$. Isto de fato é verdade. Com efeito, se fosse $r \geq b$, então $r - b = a - b \cdot q - b = a - (q + 1) \cdot b \geq 0 \Longrightarrow r - b \in S$. Mas isso é um absurdo, pois sendo $b > 0$, o número $r - b$ é menor do que r, que é o elemento mínimo de S. Portanto, deve-se ter $r < b$. Garantimos então a existência de q e r com $a = b \cdot q + r$ e $0 \leq r < b$.

2ª etapa: Para provar que q e r, com as propriedades mencionadas anteriormente, são únicos, suporemos a existência de outro par de inteiros q_1, r_1 possuindo as mesmas propriedades de q e r. Ou seja, tais que $a = b \cdot q_1 + r_1$, com $0 \leq r_1 < b$. Assim sendo, teremos:

$$b \cdot\ q_1 + r_1 = b \cdot q + r \Longrightarrow b \cdot (q_1 - q) = r - r_1 \quad (1)$$

Dessa igualdade segue que $b| r - r_1$. Porém, como $0 \leq r < b$ e $0 \leq r_1 < b$, temos que $0 \leq r < b$ e $-b < -r_1 \leq 0$. Donde segue que:

$r - b < r - r_1 \leq r \Longrightarrow -b \leq r - b < r - r_1 \leq r < b \Longrightarrow -b < r - r_1 < b \Longrightarrow |r - r_1| < b.$

Desta forma, temos que $b| r - r_1$ e $|r - r_1| < b$. Segue da propriedade (iv) do Teorema 3.2 que $r - r_1 = 0 \Longrightarrow r = r_1$. O que acarreta, de (1), que $q_1 = q$, pois $b \neq 0$.

Provamos assim que, se existem outros inteiros q_1 e r_1 possuindo as mesmas propriedades de q e r, então $q_1 = q$ e $r_1 = r$. Isso garante que q e r são únicos.

Para finalizar a prova, vamos supor o caso em que $b < 0$. Neste caso, $t = |b| > 0$. Pelo que já provamos, existem únicos $s, r \in \mathbb{Z}$ com $a = |b| \cdot s + r$ e $0 \leq r < |b|$. Isso nos dar $a = b \cdot (-s) + r$ e $0 \leq r < |b|$. Tomando $q = -s$, temos garantida a existência e unicidade de q e r, tais que $a = b \cdot q + r$ e $0 \leq r < |b|$ quando $b < 0$. Isto conclui a prova do teorema. ■

3.1.4 Máximo divisor comum entre números inteiros

Nesta seção abordaremos o conceito de máximo divisor comum entre dois inteiros e suas propriedades mais importantes.

Definição 3.4 Sejam dados dois inteiros a e b. Um divisor comum de a e b é um inteiro $d \neq 0$ que divide a e b ao mesmo tempo.

Exemplo 3.2 O 5 é um divisor comum de 25 e 60, pois 5|25 e 5|60.

Observação 3.2 Ao mencionar divisor de um número inteiro, estamos nos referindo aos divisores positivos. Uma vez que estamos interessados no máximo divisor comum, será suficiente se ater apenas aos positivos.

Antes de definirmos o máximo divisor comum de dois inteiros, apresentaremos um exemplo que ilustra este conceito. Consideremos os números 60 e 24. Sejam $D(60)$ e $D(24)$ os conjuntos dos divisores positivos de 60 e 24, respectivamente. Logo,

$$D(60) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\} \text{ e}$$

$$D(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

Observando os dois conjuntos, vemos que os divisores comuns de 60 e 24 são 1, 2, 3, 4, 6 e 12. Como 12 é o maior número dessa lista, dizemos que 12 é o máximo divisor comum de 60 e 24. Indicamos isso com a notação $mdc(60, 24) = 12$. Com esse exemplo em mente fica fácil interpretar a definição a seguir:

Definição 3.5 Sejam a e b números inteiros, com $a \neq 0$ ou $b \neq 0$. Um número inteiro $d > 0$ será dito o máximo divisor comum (mdc) de a e b se possuir as seguintes propriedades:
(i) d é divisor comum de a e b. Ou seja, $d|a$ e $d|b$.
(ii) d é o maior divisor comum de a e b. Ou seja, dado qualquer divisor c de a e b, tem-se que $c \leq d$.
Usaremos a notação $d = mdc(a, b)$ para indicar que d é o máximo divisor comum de a e b.

Vejamos algumas propriedades básicas do máximo divisor comum:

Proposição 3.1 Valem as seguintes propriedades para o máximo divisor comum de dois inteiros:
(1) (*Outra caracterização do máximo divisor comum*) O máximo divisor comum $d \neq 0$ de a e b é tal que: $d|a$ e $d|b$ e para todo divisor comum c de a e b, vale que $c|d$. Ou seja, d é divisor comum de a e b e é divisível por todo divisor comum de a e b. Esta propriedade também poderia ser usada para definir o mdc de dois inteiros, sendo equivalente a Definição 3.5. Uma demonstração deste fato pode ser encontrada em Santos (2014);

(2) (*Existência e unicidade do mdc*) Sejam a e b números inteiros, com $a \neq 0$ ou $b \neq 0$. Existe e é único o máximo divisor comum de a e b. De fato, o conjunto dos divisores comuns de a e b é não vazio (pelo menos o 1 pertence a ele) e limitado superiormente (em vista da Propriedade (iv), Teorema 3.2). Logo, o princípio da boa ordenação (versão para subconjuntos limitados superiormente) assegura que existe e é único o maior elemento desse conjunto. Esse elemento é o $mdc(a, b)$;

(3) (*Teorema de Bachet-Bézout*[25]) Seja $d = mdc(a, b)$. Existem inteiros x e y, tais que, $d = ax + by$. Ou seja, esta propriedade diz que podemos escrever o $mdc(a, b)$ como combinação linear (com coeficientes inteiros) dos inteiros a e b. Além disso, "o $mdc(a, b)$ é

[25] Ver página 20 de Martinez *et al*. (2013)

o menor inteiro positivo da forma $ax + by$" (ALENCAR FILHO, 1989, p. 87). Veja Santos (2014) ou Alencar Filho (1989) para uma demonstração pelo princípio da boa ordenação (Teorema 3.1).

(4) (*Inteiros primos entre si*) Dois inteiros a e b ($a \neq 0$ ou $b \neq 0$) são ditos primos entre si se $mdc(a, b) = 1$. Um resultado importante relacionado com essa definição é o seguinte: os inteiros a e b ($a \neq 0$ ou $b \neq 0$) são primos entre si se, e somente se, existem inteiros x e y, tais que, $ax + by = 1$.

Demonstração: De fato, se $mdc(a, b) = 1$, então a propriedade anterior garante que existem inteiros x e y, tais que, $1 = mdc(a, b) = ax + by$. Por outro lado, suponhamos que existem inteiros x e y, tais que, $ax + by = 1$ e seja $d = mdc(a, b)$. Logo, pelo item (vi) do Teorema 3.2, $d|\ (ax + by)$ para quaisquer $x, y \in \mathbb{Z}$, assim segue que $d|1 \Longrightarrow d = \pm 1$. Sendo d positivo, temos $d = 1$, o que acarreta $mdc(a, b) = 1$.

(5) (*Euclides*) Outra propriedade importante, devida a Euclides, assegura que se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.

Demonstração: De fato, se $a|b \cdot c$, então $b \cdot c = a \cdot q$, com $q \in \mathbb{Z}$. Como $mdc(a, b) = 1$, a Propriedade (3) assegura que existem inteiros x e y, tais que, $ax + by = 1$. Multiplicando esta última equação por c, vem:

$$a \cdot c \cdot x + b \cdot c \cdot y = c \Longrightarrow a \cdot c \cdot x + a \cdot q \cdot y = c \Longrightarrow a \cdot (c \cdot x + q \cdot y) = c$$

Desta última igualdade segue que $a|c$, pois $c \cdot x + q \cdot y$ é um número inteiro.

(6) Dados os inteiros a, b e y, é válido que $mdc(a, b) = mdc(a, b + y \cdot a)$. Esta propriedade auxilia muito no cálculo do mdc, pois é uma maneira de simplificar as contas.

Demonstração: De fato, se $d = mdc(a, b)$, então $d|a$ e $d|b$. Isso implica que $d|b$ e $d|y.a$ $\Longrightarrow d|(b + y \cdot a)$. Assim, $d|a$ e $d|(b + y \cdot a)$. Isso nos diz que d é divisor comum de a e $b + y \cdot a$. Para provar que $d = mdc(a, b + y \cdot a)$, seja c um divisor comum de a e $b + y \cdot a$. Logo, $c|y \cdot a$ e $c|(b + y \cdot a - y \cdot a) \Longrightarrow c|a$ e $c|b$. Assim, c é um divisor comum de a e b. Como $d = mdc(a, b)$, devemos ter $c \leq d$. Portanto, d é o maior divisor comum de a e de $b + y \cdot a$. Ou seja, $d = mdc(a, b + y \cdot a)$. ■

3.1.5 O algoritmo de Euclides

O algoritmo de Euclides consiste de um método sistemático para calcular com eficiência o máximo divisor comum de dois inteiros a e b. Este algoritmo também é conhecido como método das divisões sucessivas. Antes de apresentá-lo, provaremos um resultado que será fundamental para o seu desenvolvimento.

Teorema 3.4 Sejam a e b números inteiros com $a = b \cdot q + r$, onde q e r também são números inteiros. Temos que $mdc(a, b) = mdc(b, r)$.
Demonstração: Com efeito, $mdc(a, b) = mdc(b \cdot q + r, b) = mdc(b, r)$ pela Propriedade 6, dada anteriormente. ■

Agora, sejam a e b números inteiros, com $a \neq 0$ ou $b \neq 0$. Nosso objetivo é calcular o valor de $mdc(a, b)$. Ora, se um desses dois números é 0, então é fácil calcular o máximo divisor comum entre eles, pois $mdc(a, 0) = |a|$ e $mdc(0, b) = |b|$. Da mesma forma, se for $a = b$, então $mdc(a, b) = |a| = |b|$. Por fim, também é fácil concluir que se $a|b$, então $mdc(a, b) = |a|$. Enfim, em todas essas possibilidades o cálculo do máximo divisor comum é direto e não apresenta nenhuma dificuldade. Assim sendo, vamos supor que a e b são ambos inteiros positivos, com $a > b$, e que b não divida a. Utilizando o algoritmo da divisão (Teorema 3.3) para dividir a por b, obtemos:

$$a = b \cdot q_1 + r_1 \, , 0 < r_1 < b.$$

Em seguida, dividimos b por r_1, obtendo:

$$b = r_1 \cdot q_2 + r_2 \, , 0 \leq r_2 < b.$$

Se for $r_2 = 0$, o algoritmo pára, pois o Teorema 3.4 garantirá que

$$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = mdc(r_1, 0) = r_1.$$

Se for $r_2 > 0$, repetimos o processo e dividimos r_1 por r_2, obtendo:

$$r_1 = r_2 \cdot q_3 + r_3 \, , 0 \leq r_3 < b.$$

Pensando como anteriormente, temos que se $r_3 = 0$, então

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = mdc(r_2,r_3) = mdc(r_2,0) = r_2.$$

Por outro lado, se for $r_3 > 0$, repetimos os cálculos feitos anteriormente, chegando a:

$$r_2 = r_3 \cdot q_4 + r_4\,, 0 \leq r_4 < b.$$

Repetimos todo o processo feito nos passos anteriores e assim por diante. Nesse processo de divisões sucessivas, chegamos a duas conclusões muito importantes: a primeira é que esse processo não ocorre infinitamente. Ele pára em algum momento, pois a cada passo obtemos um resto r_j que é cada vez menor, mas não pode decrescer infinitamente porque é um número inteiro não negativo (o último resto obtido é 0). A segunda conclusão é que o $mdc(a,b)$ será igual ao último resto não nulo nessa sequência de divisões sucessivas. Para ver isso basta proceder como fizemos anteriormente, aplicando o Teorema 3.4 em cada uma das divisões que aparecem no processo. Este método para calcular o máximo divisor comum de dois inteiros é devido a Euclides e constitui-se de um dos algoritmos mais antigos em teoria dos números. Uma exposição detalhada desse algoritmo pode ser encontrada em qualquer bom livro de teoria dos números. Destacamos o livro do Coutinho (2005) que trás uma apresentação bem rica, com demonstrações e uma explicação nos mínimos detalhes desse algoritmo, apresentando ainda uma versão mais geral do mesmo, conhecido como *algoritmo euclidiano estendido*[26].

3.1.6 Números Primos

Os números primos são extremamente importantes para a criptografia de chave pública. Eles estão presentes na segurança de vários algoritmos de criptografia desse tipo. Um desses algoritmos é o RSA que apresentaremos ao final deste capitulo[27]. Conceitos relacionados com números primos, tais como fatoração, geração e critérios de primaridade,

[26] Este algoritmo é usado para determinarmos inteiros x e y, tais que $mdc(a,b) = ax + by$. Lembre-se que de acordo com a Propriedade 3 da Seção 3.1.4 esses inteiros sempre existem. O algoritmo de Euclides estendido encontra grande aplicação na resolução de equações diofantinas e congruências lineares. Faremos uma rápida apresentação das congruências lineares na seção sobre aritmética modular, mas não estudaremos as equações diofantinas detalhadamente. Sugerimos ao leitor pesquisar sobre o tema em qualquer uma das referencias citadas sobre teoria dos números.

[27] Outro algoritmo de criptografia de chave pública relacionado com números primos é o *ElGamal*. Este algoritmo se baseia no problema do logaritmo discreto para programar sua segurança. Ver: Buchmann (2002) e Terada (2000).

estão no centro da segurança do algoritmo RSA. No entanto, explorar e analisar mais ao fundo essa relação levaria muito tempo e nos obrigaria a tratar de coisas que não convêm aos nossos objetivos. Portanto, exploraremos apenas o que for necessário para a compreensão da nossa apresentação sobre o método RSA. Para isso, faremos uma exposição básica sobre números primos, destacando sua definição e alguns resultados elementares importantes. Para o leitor interessado em aprofundar seus estudos sobre números primos e criptografia RSA, sugerimos a consulta das seguintes obras que abarcam o tema de modo amplo e bem acessível ao público leigo: Daineze (2013), Okumura (2014), Spina (2014), Sousa (2015) e outras já citadas, tais como Medeiros (2017), Coutinho (2005) e Carneiro (2017). Os livros de Terada (2000) e Buchmann (2002) tratam de um estudo mais aprofundado e teórico sobre criptografia, em particular da criptografia de chave pública que destaca os números primos como agente principal de sua segurança. Para conhecer a história dos números primos e do seu desenvolvimento ao longo do tempo, o leitor pode consultar Sautoy (2007). A obra de Sautoy também dedica um capítulo ao estudo de criptografia de chave pública e números primos, bem como elementos de teoria dos números.

Definição 3.6: Um inteiro positivo p $(p > 1)$ é chamado de número primo quando seus únicos divisores positivos são 1 e p. Se p não for primo, ele será chamado de composto.

Exemplo 3.3 Os números 2, 3, 5, 7, 11, 13, 17 e 19 são todos primos. Já os números 8, 10, 15, 18, 28, 30 e 40 são compostos.

Observação 3.3 O número natural 1 nem é primo e nem composto. O número 2 é o único número primo par. Logo, se p é primo e maior do que 2, então p é impar.

Teorema 3.5 Seja p um número primo e a um inteiro qualquer. Se $p \nmid a$, então $mdc(a, p) = 1$. Ou seja, a e p são primos entre si. Consequentemente, se a e b são inteiros quaisquer e $p|a \cdot b$, então $p|a$ ou $p|b$.

Demonstração: Com efeito, seja $d = mdc(a, p)$. Logo, $d|a$ e $d|p$. Ora, como $d|p$ e p é primo, concluímos que só há dois valores possíveis para d: 1 ou p. Se $d = p$, então teríamos $p|a$, pois $d|a$, o que contradiz a hipótese de que $p \nmid a$. Portanto, devemos ter $d = 1$. Assim, temos $mdc(a, p) = 1$.

Suponhamos agora que $p|a \cdot b$. Se $p \nmid a$, então $mdc(a,p) = 1$ pelo que já provamos. Logo, pela propriedade de Euclides (Propriedade 5 sobre máximo divisor comum) segue que $p|b$. Ou seja, se p divide o produto $a \cdot b$, então ele deve dividir ao menos um dos fatores. ■

Exemplo 3.4 O 5 é um número primo e $5 \nmid 27$. Logo, $mdc(5,27) = 1$. Da mesma forma, veja que $5|4 \cdot 10 \Longrightarrow 5|4$ ou $5|10$ (o que é verdade pois $5|10$).

A segunda afirmação contida no Teorema 3.5 pode ser generalizada para uma quantidade finita n de inteiros. Ou seja, se p é um número primo, onde $p|a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n$ ($a_i \in \mathbb{Z}$), então existe um inteiro a_k ($1 \leq k \leq n$), tal que, $p|a_k$. Um resultado mais particular assegura que se $a_1, a_2, a_3, \ldots, a_n$ forem também primos, então existirá um índice j ($1 \leq j \leq n$) tal que $p = a_j$. Ou seja, se um número primo divide um produto de números primos, então ele deve ser igual a um dos fatores. Veja o Capítulo 7 de Alencar Filho (1989).

Baseando-se em Alencar Filho (1989), apresentaremos e demonstraremos a seguir o Teorema Fundamental da Aritmética (TFA). Um dos teoremas mais simples e importantes da teoria dos números. Sua simplicidade faz com que o mesmo seja um dos poucos teoremas da aritmética básica que ainda é estudado no ensino básico. Para demonstrarmos esse teorema, faremos uso do seguinte resultado.

Lema 3.1 Todo número composto possui ao menos um divisor primo.

Demonstração: Mais precisamente, provaremos que o menor divisor de um inteiro composto n é primo. De fato, seja p o menor divisor de n. Se p fosse composto, poderíamos escrever $p = r \cdot s$, com $1 < r, s < p$. Logo, como r e s são divisores de p, segue que r e s são divisores de n. Mais isso é absurdo, porque r e s são menores do que p, e p é o menor divisor de n.■

Teorema 3.6 (*Teorema Fundamental da Aritmética*) Todo inteiro positivo n ($n > 1$) pode ser escrito como um produto de números (fatores) primos. Esse produto é único, a não ser pela ordem dos fatores. Assim sendo, todo inteiro positivo maior do que 1 ou é primo ou pode se escrever como produto de números primos.

Demonstração:

(*Existência*) Suponhamos n composto (se ele for primo, nada há para demonstrar). Pelo lema anterior, n possui um divisor primo p_1. Logo, $n = p_1 \cdot k_1$, com $1 < k_1 < n$. Ora, se k_1 for primo, a demonstração acaba e temos que $n = p_1 \cdot k_1$. Por outro lado, se k_1 for composto, novamente pelo lema anterior temos que $k_1 = p_2 k_2$, com p_2 primo e $1 < k_2 < k_1$. Logo, $n = p_1 \cdot p_2 \cdot k_2$. Podemos fazer uma análise semelhante sobre k_2 e repetir os passos anteriores. Seguido assim, obtemos uma sequência de inteiros:

$$n > k_1 > k_2 > k_3 > k_4 > \cdots > 1.$$

Como essa é uma sequência decrescente de inteiros maiores do que 1, segue que a mesma é finita. Existe, então, um último k_j que será menor do que todos os outros. Portanto, k_j é primo e podemos escrever $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r$ $(p_r = k_j)$, onde todos os $p_i´s$ são primos. Assim, provamos que n pode ser escrito como um produto de fatores primos.

(*Unicidade*) Para provar que essa maneira de escrever n é única, vamos supor que n admite outra representação como produto de números primos. Seja $n = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_s$, onde $q_i \leq q_j \; se \; i < j$. Provaremos que $r = s$ e $p_i = q_i (1 \leq i \leq r)$. Para isso, suponhamos por absurdo que $r \neq s$. Sem perda de generalidade, podemos supor que $r < s$. Temos então o seguinte:

Como $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_s$, segue que $q_1 | p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r$. Pela observação após o Teorema 3.5, concluímos que $q_1 = p_j \geq p_1$, para algum $1 \leq j \leq r$. Da mesma forma, $p_1 | q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_s$. Logo, $p_1 = q_i \geq q_1$, para algum $1 \leq i \leq s$. Portanto,

$$p_1 = q_1 \Longrightarrow p_2 \cdot p_3 \cdot \ldots \cdot p_r = q_2 \cdot q_3 \cdot \ldots \cdot q_s.$$

Repetindo este processo, obtemos $p_2 = q_2$, $p_3 = q_3$ e assim por diante. Supondo que $r < s$, temos que na igualdade $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_s$ o lado direito tem mais fatores do que o esquerdo. Logo, se formos eliminando os pares $p_l = q_k$ de primos iguais, chegaremos à igualdade $1 = q_{r+1} \cdot q_{r+2} \cdot q_{r+3} \cdot \ldots \cdot q_s$. Como no lado direito dessa igualdade temos um produto de números primos, esse produto não pode ser 1. Logo, a igualdade dada por $1 = q_{r+1} \cdot q_{r+2} \cdot q_{r+3} \cdot \ldots \cdot q_s$ é absurda. Concluímos assim que devemos ter $r = s$. Isso nos diz que $p_1 = q_1, p_2 = q_2, p_3 = q_3, \ldots, p_r = q_r$. Ou seja, é única a forma para $n = p_1 . p_2 . p_3 \ldots p_r$. Provamos assim a existência e unicidade da representação de n como produto de fatores primos. Isto conclui a demonstração. ■

Observação 3.4 É claro que quando escrevemos $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r$, os fatores primos $p_1, p_2, p_3, \ldots, p_r$ não são necessariamente distintos. Assim, organizando esses fatores primos

em ordem crescente e agrupando os fatores iguais, se existirem, pode-se escrever $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_r^{n_r}$, com $p_1 < p_2 < p_3 < \cdots < p_r$ e $n_i > 0$ para todo $1 \leq i \leq r$. Esta é a chamada fatoração (ou decomposição) canônica de n.

Exemplo 3.5 Seja $n = 340$. Temos que

$$n = 340 = 34 \cdot 10 = 2 \cdot 17 \cdot 2 \cdot 5 = 2^2 \cdot 5 \cdot 17.$$

Portanto, $2^2 \cdot 5 \cdot 17$ é a decomposição canônica de 340.

O teorema a seguir foi provado pela primeira vez por Euclides. O mesmo assegura que os números primos jamais se esgotarão. A demonstração apresentada segue a prova clássica dada por Euclides há mais de 2000 mil anos.

Teorema 3.7 Existem infinitos números primos.

Demonstração: Com efeito, suponhamos por absurdo que o conjunto dos números primos é finito. Assim sendo, sejam $p_1, p_2, p_3, \ldots, p_k$ a lista de todos os números primos. Se considerarmos o número $P = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$, que é o número obtido pela multiplicação de todos os primos da lista apresentada acrescido de uma unidade, então P será maior do que 1 e não será divisível por nenhum dos primos $p_1, p_2, p_3, \ldots, p_k$. O Teorema Fundamental da Aritmética garante que ou P é primo ou pode ser escrito como produto de números primos. Ora, se P for primo, ele não pode pertencer a nossa lista, pois P é maior do que todos os $p_i's$. Por outro lado, se P puder ser escrito como produto de números primos, então ele será divisível por todos os primos que compõe esse produto. Logo, nenhum primo desse produto será igual a algum primo da lista $p_1, p_2, p_3, \ldots, p_k$. Ou seja, existem outros primos que geram P. Portanto, em qualquer das possibilidades para P, temos garantida a existência de outros primos que não pertencem a lista $p_1, p_2, p_3, \ldots, p_k$. Esta contradição mostra que a lista dos números primos não pode ser finita. ■

O fato de existir infinitos primos é o que fornece mais subsídios para a segurança do método criptográfico RSA. De fato, como veremos mais adiante, este método se alimenta de números primos para construir suas chaves de segurança. Utilizar números primos cada vez maiores, com um número muito grande de algarismos é o que pode dar maior segurança e menores probabilidades do sistema ser violado.

Antes de analisarmos onde os números primos estão inseridos no método RSA, precisamos estudar alguns conceitos relacionados à aritmética modular. Os processos de codificação, decodificação, geração de chaves, funcionamento geral, segurança, entre outros, referentes ao método RSA se utilizam de alguma noção dessa área, mais precisamente a noção de inteiros congruentes. É essencial, portanto, conhecer um pouco sobre aritmética modular para entender o conteúdo que será desenvolvido posteriormente.

3.1.7 Aritmética Modular

Discutiremos agora sobre algumas noções de aritmética modular. Também conhecida como aritmética do relógio, a aritmética modular insere no conjunto dos números inteiros uma espécie de *fenômeno cíclico*, o qual estabelece uma relação entre dois inteiros e possibilita classificá-los como *congruentes* em relação a outro número inteiro. A aritmética modular foi inicialmente desenvolvida pelo eminente matemático alemão Carl Friedrich Gauss (1777-1855), tomando como ponto de partida a idealização de uma *calculadora-relógio.*

> Uma das grandes contribuições precoces de Gauss foi a invenção da calculadora-relógio. Esse instrumento era uma ideia, e não uma máquina física, que possibilitava a realização de cálculos com números considerados demasiadamente extensos. O princípio da calculadora-relógio é idêntico ao de um relógio comum. Se um relógio marca nove horas, e adicionamos quatro horas, o ponteiro das horas avança até uma hora. Assim, a calculadora-relógio de Gauss nos daria a resposta 1, e não 13. (SAUTOY, 2007, p. 29)

Para a multiplicação $7 \cdot 7$ digamos, o valor fornecido pela calculadora – relógio de Gauss seria 1, pois este é o resto na divisão de $7 \cdot 7 = 49$ por 12. Diante disso, ficava ainda mais fácil para Gauss obter, por exemplo, o valor de $7 \cdot 7 \cdot 7$. Como $7 \cdot 7$ é igual a 1 na sua calculadora, para obter o valor de $7 \cdot 7 \cdot 7$, Gauss só precisava multiplicar 1 por 7. Logo, sua calculadora lhe fornecia o valor 7, isto é, o número $7 \cdot 7 \cdot 7$ deixa resto 7 na divisão por 12. A eficiência e a velocidade de cálculo da calculadora-relógio de Gauss tornaram-se claros ao serem realizadas multiplicações com um número maior de fatores: “embora não tivesse a menor ideia do valor de 7^{99}, sua calculadora-relógio lhe dizia que o número deixava resto 7 ao ser dividido por 12” (SAUTOY, 2007, p. 29).

Evidentemente, os relógios com 12 horas não tinham nada de especial e a ideia da calculadora – relógio de Gauss poderia ser aplicada a um relógio com uma quantidade *m* de

horas. Ao generalizar essa ideia para relógios com uma quantidade qualquer de horas, Gauss deu vida a uma nova aritmética. Uma aritmética sobre os restos obtidos na divisão de inteiros, que está fixada na noção fundamental de *congruência.* O potencial dessa nova aritmética reside justamente nessa noção de congruência que torna possível a realização de divisões com números gigantescos em uma velocidade muito grande. Sem contar que as congruências são dotadas de uma aritmética muito simples, cujas propriedades se assemelham muito com as da relação de igualdade. Certamente a aritmética modular foi uma das grandes contribuições de Gauss, que proporcionou o desenvolvimento não só da teoria dos números, mas de toda a matemática. Segundo Sautoy (2007, p. 29), "a descoberta desse novo tipo de aritmética revolucionou a matemática na virada do século XIX. [...] a invenção da calculadora-relógio ajudou os matemáticos a descobrir padrões no universo dos números, que haviam estados escondidos durante gerações".

Em pleno século XXI, a aritmética modular de Gauss representa a ferramenta mais poderosa para o desenvolvimento da criptografia moderna na internet. Essa aritmética é o alicerce para muitos sistemas de criptografia, especificamente criptografia de chave pública. O mais famoso desses sistemas é, como já falamos, o RSA. Muitos resultados e conceitos relacionados com congruências estão inseridos no funcionamento desse método. Portanto, iremos estudar algumas noções sobre aritmética modular com o intuito de preparar o terreno para a apresentação do método RSA. Faremos a apresentação de algumas definições e resultados importantes que estão relacionados diretamente, ou indiretamente, com o RSA. Iniciaremos com a importante noção de inteiros congruentes.

Definição 3.7 (*Inteiros congruentes*) Sejam a, b e m números inteiros, com $m > 0$. Diremos que a é congruente a b módulo m quando $a - b$ for múltiplo de m, isto é, quando $m|a - b$.

Pode-se provar que a definição anterior é equivalente a seguinte: a é congruente a b módulo m se, e somente se a e b deixam o mesmo resto quando divididos por m. Usaremos a notação $a \equiv b\ (mod. m)$ para indicar que a é congruente a b módulo m. Assim, temos: $a \equiv b\ (mod. m) \Leftrightarrow\ m|a - b \Leftrightarrow\ a\ e\ b$ deixam o mesmo resto quando divididos por m.

Exemplo 3.6 Temos $7 \equiv 1\ (mod. 3)$, pois $3|(7 - 1)$; $-15 \equiv 9\ (mod. 8)$, pois $8|(-15 - 9)$; $11 \equiv -1(mod. 4)$, pois $4|(11 - (-1))$; $n \equiv 0\ (mod. 2)$ para qualquer n par; $n \equiv 1\ (mod. 2)$, para todo n ímpar; como 17 = 4.4 + 1 e 29 = 4.7 + 1, segue que 17 e 29 deixam o mesmo resto quando divididos por 4. Portanto, $17 \equiv 29\ (mod. 4)$.

Quando $m \nmid a - b$, dizemos que a é incongruente a b módulo m. Indicamos isso com a notação $a \not\equiv b\ (mod.m)$. Isso quer dizer que a e b não deixam o mesmo resto quando divididos por m.

Exemplo 3.7 Temos $7 \not\equiv 2\ (mod.3)$, pois $3 \nmid (7-2)$; $-4 \not\equiv 1\ (mod.7)$, pois $7 \nmid (-4-1)$ e $19 \not\equiv 11\ (mod.5)$, pois $5 \nmid (19-11)$

Observação 3.5

- Como $1|(a-b)$ para todos a e b inteiros, segue então que $a \equiv b\ (mod.1)$. Por esse motivo podemos descartar a congruência módulo 1 e supor sempre $m > 1$;
- A relação "a congruente a b módulo m" é de equivalência em $\mathbb{Z}$. Isto significa que para todos a, b, c e m inteiros, com $m > 1$, valem as seguintes propriedades:
  (1) $a \equiv a\ (mod.m)$ (*propriedade reflexiva*);
  (2) Se $a \equiv b\ (mod.m)$, então $b \equiv a\ (mod.m)$ (*propriedade simétrica*);
  (3) Se $a \equiv b\ (mod.m)$ e $b \equiv c\ (mod.m)$, então $a \equiv c\ (mod.m)$ (*propriedade transitiva*).
- (C*aracterização do resto*) O problema de obter o resto na divisão de um inteiro a por $m > 0$ é equivalente ao de obter um inteiro r, com $0 \leq r < m$, tal que $a \equiv r\ (mod.m)$. Assim, por exemplo, se quisermos calcular o resto de 9^{100} por 17, basta encontrar um número $0 \leq r < 17$ que verifique $9^{100} \equiv r\ (mod.17)$.

As duas últimas observações citadas anteriormente são consequências imediatas da definição de inteiros congruentes. Suas demonstrações não apresentam nenhuma dificuldade e serão deixadas como exercício. Os teoremas a seguir destacam algumas propriedades úteis das congruências.

Teorema 3.8 Sejam dados os números inteiros a, b, c, d e m, com $m > 1$. Então:

(1) Se $a \equiv b\ (mod.m)$, então $a \cdot c \equiv b \cdot c\ (mod.m)$. Ou seja, nas congruências é permitido multiplicar ambos os membros por um mesmo número inteiro;

(2) Se $a \equiv b\ (mod.m)$ e n é um inteiro divisor de m, então $a \equiv b\ (mod.n)$;

(3) Se $a \equiv b\ (mod.m)$ e $c \equiv d\ (mod.m)$, então

$$a + c \equiv b + d\ (mod.m) \text{ e } a - c \equiv b - d\ (mod.m)\ .$$

Consequentemente, temos que $a + c \equiv b + c\ (mod.m)$ e $a - c \equiv b - c\ (mod.m)$. Esta propriedade diz que as congruências módulo m podem ser somadas e subtraídas membro a membro, bem como podemos somar e subtrair um mesmo número inteiro em ambos os membros de uma congruência;

(4) Se $a \equiv b\ (mod.m)$, então para todo $n \in \mathbb{N}$, vale que $a^n \equiv b^n (mod.m)$.

As demonstrações dessas propriedades não apresentam nenhuma dificuldade e serão omitidas. Tais demonstrações podem ser consultadas em Santos (2014).

O teorema a seguir destaca uma propriedade muito importante das congruências. Nas igualdades entre números reais, por exemplo, do tipo $ax = ay$, só podemos cancelar o fator comum a desde que ele seja diferente de zero. Nas congruências há também uma condição para que possamos cancelar um fator comum de ambos os membros. Essa condição assegura que só podemos cancelar o fator comum desde que ele seja primo com o módulo.

Teorema 3.9 Seja $a \cdot c \equiv b \cdot c\ (mod.m)$ e c primo com m. Então $a \equiv b\ (mod.m)$, isto é, o fator c pode ser cancelado.

Demonstração: Com efeito, desde que $a \cdot c \equiv b \cdot c\ (mod.m)$, podemos garantir que $m|(a \cdot c - b \cdot c)$. Daí, pondo o fator c em evidência, obtemos: $m|c \cdot (a - b)$. Como c é primo com m, isto significa que $mdc(c, m) = 1$. Portanto, o Teorema de Euclides (dado como Propriedade 5 na Seção 3.1.4) garante que $m|a - b$, donde $a \equiv b\ (mod.m)$. ■

Exemplo 3.8 Considere a congruência $36 \equiv 12\ (mod.3)$. Como $36 = 2 \cdot 18$ e $12 = 2 \cdot 6$, temos $2 \cdot 18 \equiv 2 \cdot 6\ (mod.3)$. Como $mdc(2,3) = 1$, segue que $18 \equiv 6\ (mod.3)$.

A definição a seguir estabelece uma noção muito presente em criptografia RSA. Trata-se da noção de inverso multiplicativo de um inteiro módulo m. Sabemos que inverso multiplicativo é um conceito relacionado à multiplicação, em $\mathbb{R}$, por exemplo, o qual estabelece que um número b é o inverso multiplicativo de a se, e somente se $a \cdot b = 1$. Em termos de congruências, temos o seguinte.

Definição 3.8 Sejam a e m números inteiros, com $m > 1$. Um número inteiro b é dito inverso multiplicativo de a módulo m se $a \cdot b \equiv 1\ (mod.m)$. Esse inverso multiplicativo módulo m, quando existe, é único, módulo m.

Denota-se por a^{-1} o inverso multiplicativo de a. Daí, multiplicando os dois lados da congruência $a \cdot b \equiv 1\ (mod.m)$ por a^{-1}, teremos: $a \cdot b \cdot a^{-1} \equiv 1 \cdot a^{-1}\ (mod.m)$. Logo. $b \cdot (a \cdot a^{-1}) \equiv a^{-1}(mod.m) \Longrightarrow b \equiv a^{-1}(mod.m)$. Isto justifica o fato do inverso módulo m ser único.

Exemplo 3.9 Temos que o inverso multiplicativo de 4 módulo 7 é 2, pois $4 \cdot 2 \equiv 1\ (mod.7)$. Veja que qualquer inteiro c, com $c \equiv 2\ (mod.7)$ é um inverso multiplicativo de 4 módulo 7. Veja também que 4 é primo com 7. Isso não é por acaso. A fim de que a possua inverso multiplicativo módulo m é necessário e suficiente que a seja primo com m. Este é o conteúdo do Teorema 3.10 a seguir.

Teorema 3.10 Sejam a e m, $m > 1$, inteiros quaisquer. Existe um inteiro b, tal que $a \cdot b \equiv 1\ (mod.m)$ se, e somente se, $mdc\ (a, m) = 1$.

Demonstração: De fato, suponhamos que exista $b \in \mathbb{Z}$, tal que $a \cdot b \equiv 1\ (mod.m)$. Logo, $m|(a \cdot b - 1)$. Daí, existe um número $k \in \mathbb{Z}$, tal que $a \cdot b - 1 = m.k \Longrightarrow a \cdot b - m \cdot k = 1$. Seja $d = mdc(a, m)$, então $d|a$ e $d|m \Longrightarrow d|a \cdot b$ e $d|m \cdot k \Longrightarrow d|a \cdot b - m \cdot k \Longrightarrow d|1$, donde $d = 1$, pois $d > 0$. Portanto, $mdc(a, m) = 1$.

A recíproca é óbvia, uma vez que se $mdc(a, m) = 1$, então existem $x, y \in \mathbb{Z}$, com $ax + my = 1 \Longrightarrow ax - 1 = m \cdot (-y) \Longrightarrow m|(ax - 1) \Longrightarrow ax \equiv 1\ (mod.m)$. Portanto, x é o inverso multiplicativo de a módulo m. ■

Definição 3.9 Seja x um número inteiro. Chama-se resíduo de x módulo m um inteiro a, tal que, $x \equiv a\ (mod.m)$.

Exemplo 3.10 5 é um resíduo de 12 módulo 7, pois $12 \equiv 5\ (mod.7)$.

Dado um inteiro $m > 1$, há uma quantidade finita de resíduos, incongruentes entre si, módulo m. Podemos considerar o conjunto de todos esses resíduos. Isso nos leva a definir o conceito de *Sistema Completo de Resíduos Módulo* m. Intuitivamente, um sistema completo

de resíduos é um conjunto cujos elementos são todos os resíduos, incongruentes dois a dois, possíveis a módulo m. Dois resíduos congruentes módulo m são considerados iguais com relação a esse módulo. Portanto, ser incongruentes dois a dois significa que esses resíduos são distintos[28]. Precisamente, um sistema completo de resíduos módulo m é um conjunto $\{r_1, r_2, \dots, r_s\}$ de s inteiros, onde $r_i \not\equiv r_j (mod. m)$ para todo $i \neq j$ e dado qualquer número inteiro n, existe um r_i tal que $n \equiv r_i\ (mod. m)$. Pode-se provar (ver Santos (2014)) que se $\{r_1, r_2, \dots, r_s\}$ é um sistema completo de resíduos módulo m, então $s = m$.

Exemplo 3.11 O conjunto $\{0, 1, 2, 3, 4, \dots, m-1\}$ é um sistema completo de resíduos módulo m. Com efeito, é claro que esses inteiros são dois a dois incongruentes módulo m, pois se dois elementos distintos desse conjunto, digamos r e s fossem congruentes módulo m, teríamos que $m|r-s$. Como $|r-s| < m$, segue que $r - s = 0$, donde $r = s$. O que é um absurdo. Por outro lado, dado um inteiro n qualquer, temos que $n \equiv r\ (mod. m)$, onde $0 \leq r < m$. Portanto, $\{0, 1, 2, 3, 4, \dots, m-1\}$ é um sistema completo de resíduos módulo m.

Usaremos o exposto anteriormente para provar o teorema a seguir, muito importante em termos de aplicação em criptografia RSA.

Teorema 3.11 (*Pequeno Teorema de Fermat*) Seja p um número primo e a um inteiro qualquer não divisível por p. Então, $a^{p-1} \equiv 1\ (mod. p)$. Ou seja, se p é primo e p não divide a, então p divide $a^{p-1} - 1$.

Demonstração: Consideremos os conjuntos $\{0, 1, 2, 3, \dots p-1\}$ e $\{a, 2a, 3a, \dots, (p-1)a\}$. O primeiro conjunto é um sistema completo de resíduos módulo p de acordo com o exemplo anterior. Agora, o segundo conjunto tem $p-1$ elementos, nenhum dos quais é múltiplo de p. Esses elementos são incongruentes, dois a dois, módulo p. De fato, sejam ia e ja dois elementos distintos do conjunto $\{a, 2a, 3a, \dots, (p-1)a\}$, $1 \leq i, j \leq p-1$. Se fosse $ia \equiv ja\ (mod. p)$, teríamos $i \equiv j\ (mod. p)$. Como i e j são menores do que p, segue então que $i = j$. O que é absurdo. Assim sendo, podemos concluir que cada elemento do conjunto $\{a, 2a, 3a, \dots, (p-1)a\}$ é congruente a um único elemento do conjunto $\{1, 2, 3, \dots p-1\}$.

[28] Essa é uma característica geral das congruências. A noção de igualdade (ou equivalência), com relação a m, se reflete na de congruência. Defini-se, portanto, dois inteiros como distintos módulo m se eles forem incongruentes com relação a esse módulo. Isso tem uso muito frequente não só no estudo dos sistemas completos de resíduos, mas também nas equações que envolvem congruência, popularmente conhecida como congruências lineares, para estabelecer a distinção entre suas raízes.

Como esses conjuntos têm a mesma quantidade de elementos, o produto $a \cdot 2a \cdot\ 3a \cdot\ \ldots \cdot (p-1)a$ será congruente ao produto $1 \cdot 2 \cdot 3 \cdot\ \ldots \cdot p-1$. Assim, teremos:

$$a \cdot 2a \cdot\ 3a \cdot \ldots \cdot (p-1)a \equiv\ 1 \cdot 2 \cdot 3 \cdot \ldots \cdot p-1\ (mod.p)$$

$$\Longrightarrow a^{p-1} \cdot \big(1.2.3 \ldots (p-1)\big) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)(mod.p). \quad \text{(i)}$$

Como todos os elementos do conjunto $\{1, 2, 3, \ldots, p-1\}$ são menores que p, e p é primo, segue que todos eles são primos com p. Portanto, $mdc(1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1), p) = 1$ e podemos cancelar o fator $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ na congruência (i), obtendo $a^{p-1} \equiv 1\ (mod.p)$, como queríamos demonstrar. ■

Como consequência do Pequeno Teorema de Fermat, temos outro importante resultado, que também é denominado de Pequeno Teorema de Fermat por alguns autores. Este resultado afirma que se p é primo e a é um inteiro qualquer, então $a^p \equiv a\ (mod.p)$. De fato, se $p|a$ não há o que demonstrar, pois nesse $p|\ a^p - a$. Por outro lado, se $p \nmid a$, então pelo Teorema 3.11, segue que $a^{p-1} \equiv 1\ (mod.p)$. Multiplicando ambos os lados dessa congruência por a, chegamos ao resultado desejado.

Exemplo 3.12 Como 5 é primo e 5 não divide 37, segue que $37^{5-1} \equiv 1\ (mod.5)$. Daí, teremos $37^4 \equiv 1\ (mod.5)$. Da mesma forma, é sempre verdade que $37^5 \equiv 37\ (mod.5)$.

O leitor interessado pode consultar Sautoy (2007), Capítulo 10, para obter uma interpretação bem interessante do Pequeno Teorema de Fermat em termos da calculadora-relógio de Gauss, bem como uma explicação bem rica e ilustrada da ação desse teorema sobre a criptografia RSA. Esse capítulo da obra de Sautoy é dedicado à criptografia.

Iremos finalizar essa explanação sobre alguns conceitos elementares da aritmética básica abordando a importante função φ*(letra grega fi)* e o conceito de Congruências Lineares.

Definição 3.10 (*Função φ de Euler*) Seja $n \in \mathbb{N}$. A função φ de Euler é uma função aritmética[29] definida por: $\varphi(n) =$ número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n. Ou seja, $\varphi(n)$ é o número de elementos do conjunto $\{x \in \mathbb{N}; x \leq n\ e\ mdc(x, n) = 1\}$.

[29] Uma função cujo domínio e contradomínio é o conjunto $\mathbb{N}$ dos números naturais.

Exemplo 3.13 De acordo com a Definição 3.10, temos:
$\varphi(1) = 1$, pois 1 é o único inteiro positivo menor do que ou igual a 1 e primo com 1;
$\varphi(2) = 1$, pois $1 \leq 2$ e $mdc(1,2) = 1$;
$\varphi(3) = 2$, pois há dois inteiros positivos menores do que ou iguais a 3 que são primos com 3: 1 e 2.
$\varphi(10) = 4$, pois 1, 3, 7 e 9 são os únicos inteiros positivos menores do que ou iguais a 10 e primos com 10.

O teorema a seguir mostra como calcular $\varphi(n)$ quando n é primo e quando n for uma potência de um número primo.

Teorema 3.12 Seja p um número primo e a um número inteiro positivo. Vale que

$$\varphi(p) = p - 1 \text{ e } \varphi(p^a) = p^a - p^{a-1}. \quad (1)$$

Demonstração: Seja p um número primo. Os números $1, 2, 3, 4, 5, \ldots, p-1$ são todos menores do que p e relativamente primos com p, pois sendo p primo, p não divide nenhum número dessa lista. Logo, $mdc(p,i) = 1$ para $1 \leq i \leq p-1$. Portanto, há $p-1$ inteiros positivos menores do que p e primos com p, isto é, $\varphi(p) = p - 1$.
Para ver que $\varphi(p^a) = p^a - p^{a-1}$, consideremos a sequência dos inteiros positivos desde 1 até p^a: $1, 2, 3, \ldots, p^a$. Queremos saber quantos desses inteiros são primos com p. Ora, para saber isso, devemos nos perguntar quantos desses inteiros não são primos com p. Na sequência $1, 2, 3, \ldots, p^a$, os únicos números que não são primos com p são aqueles múltiplos de p, isto é, os inteiros $1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p^{a-1} \cdot p = p^a$. Daí, se subtrairmos a quantidade desses inteiros (p^{a-1}) da quantidade total de inteiros da sequência $1, 2, 3, \ldots, p^a$ (p^a), temos a quantidade de inteiros positivos menores do que ou iguais a p^a que são primos com p^a. Ou seja, $\varphi(p^a) = p^a - p^{a-1}$. ■

Exemplo 3.14 Tem-se $\varphi(13) = 13 - 1 = 12$, pois 13 é primo. Da mesma forma, temos $\varphi(7^3) = 7^3 - 7^{3-1} = 343 - 49 = 294$.

Antes de aprendermos a calcular $\varphi(n)$ para todo natural n, necessitamos de uma definição sobre uma classe particular muito importante de funções aritméticas. Trata-se das funções aritméticas multiplicativas. Chamam-se assim as funções aritméticas $f: \mathbb{N} \to \mathbb{Z}$, tais que $f(m \cdot n) = f(m) \cdot f(n)$ para todo par de inteiros positivos m, n, primos entre si. A

função φ de Euler se enquadra nessa classe de funções, isto é, $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ para todos $m, n \in \mathbb{N}$ com $mdc(m,n) = 1$. Uma prova deste fato pode ser encontrada em Santos (2014, p.72) ou em qualquer livro sobre Teoria dos Números.

Sabemos pelo Teorema Fundamental da Aritmética que todo inteiro positivo $n > 1$ pode ser escrito, de modo único, na forma $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_r^{n_r}$, com $p_1 < p_2 < \cdots < p_r$ e $n_i > 0$ para todo $1 \leq i \leq r$. Como os primos $p_i's$ são distintos, as potências $p_i^{n_i}{}'s$ são números primos entre si. Assim, para $n = 1$, já sabemos que $\varphi(1) = 1$. Por outro lado, se $n > 1$, escrevemos $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_r^{n_r}$ e aplicamos a função φ. Obtemos:

$$\varphi(n) = \varphi\left(p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_r^{n_r}\right) = \varphi\left(p_1^{n_1}\right) \cdot \varphi\left(p_2^{n_2}\right) \cdot \ldots \cdot \varphi(p_r^{n_r}).$$

Já sabemos calcular φ para potências de números primos pelo Teorema 3.12. Portanto, teremos:

$$\varphi(n) = \varphi\left(p_1^{n_1}\right) \cdot \varphi\left(p_2^{n_2}\right) \cdot \ldots \cdot \varphi\left(p_r^{n_r}\right) = \left(p_1^{n_1} - p_1^{n_1-1}\right) \cdot \left(p_2^{n_2} - p_2^{n_2-1}\right) \cdot \ldots \cdot \left(p_r^{n_r} - p_r^{n_r-1}\right)$$

$$\Longrightarrow \varphi(n) = p_1^{n_1}\left(1 - \frac{1}{p_1}\right) \cdot \; p_2^{n_2}\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot p_r^{n_r}\left(1 - \frac{1}{p_r}\right)$$

$$\Longrightarrow \varphi(n) = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_r^{n_r} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right)$$

$$\Longrightarrow \varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right). \qquad (2)$$

A Fórmula 2 nos possibilita calcular $\varphi(n)$ para todo $n > 1$. Ela requer apenas que saibamos fatorar n em seus constituintes primos. Quando estudarmos o método RSA, veremos que fatorar n está diretamente relacionado com a quebra do código. Especificamente, fatorar n e obter $\varphi(n)$, para os $n's$ que são utilizados no RSA, significará quebrar o código.

Exemplo 3.15 Vamos calcular $\varphi(2020)$. Como $2020 = 2^2 \cdot 5 \cdot 101$ é a fatoração canônica de 2020, segue da Fórmula 2 que

$$\varphi(2020) = 2020 \cdot \left(1 - \tfrac{1}{2}\right) \cdot \left(1 - \tfrac{1}{5}\right) \cdot \left(1 - \tfrac{1}{101}\right) = 2020 \cdot \tfrac{1}{2} \cdot \tfrac{4}{5} \cdot \tfrac{100}{101} = 2020 \cdot \tfrac{40}{101} = 800.$$

Ou seja, existem 800 inteiros positivos menores do que ou iguais a 2020 que são relativamente primos com 2020.

A seguir, enunciaremos o famoso Teorema de Euler (ou Teorema de Euler-Fermat), o qual é bastante usado para calcular resíduos de potências módulo m quando a base da potência é um número primo com m e a potência é relativamente grande. A demonstração desse teorema pode ser encontrada em Santos (2014, p. 43).

Teorema 3.13 Sejam a e m números inteiros, com $m > 0$ e $mdc(a, m) = 1$. Então,

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

Exemplo 3.16 Sejam dados os inteiros $a = 7$ e $m = 15$. Como $mdc(7, 15) = 1$ e $\varphi(15) = \varphi(3.5) = \varphi(3).\varphi(5) = 2.4 = 8$, segue que $7^{\varphi(15)} = 7^8 \equiv 1 \ (mod. 15)$.

Para encerrarmos esta seção, faremos algumas considerações sobre *congruências lineares*. Chamam-se assim as congruências do tipo $ax \equiv b \ (mod. m)$, onde a, b, x e m são inteiros, com $m > 0$. Veja que há uma forte semelhança entre esse tipo de congruência e as equações de primeiro grau $ax + b = 0$. Nas equações, seja de primeiro grau ou não, nosso objetivo é determinar o(s) valor(es) de x que satisfaz(em) a equação dada. Isso não é diferente com as congruências $ax \equiv b \ (mod. m)$, onde procuramos determinar $x_0 \in \mathbb{Z}$, de modo que, $ax_0 \equiv b \ (mod. m)$. Tal x_0 que verifique a congruência $ax_0 \equiv b \ (mod. m)$ será chamado de solução dessa congruência. Assim, considerando a congruência dada por $3x \equiv 1 \ (mod. 2)$, temos que $x_0 = 3$ é solução, pois $3 \cdot 3 = 9 \equiv 1 \ (mod. 2)$.

É fácil ver que, se x_0 é solução da congruência $ax_0 \equiv b \ (mod. m)$ e $x_1 \equiv x_0 \ (mod. m)$, então x_1 também é solução de $ax_0 \equiv b \ (mod. m)$. Com efeito, se temos $x_1 \equiv x_0 \ (mod. m)$, então $ax_1 \equiv ax_0 \equiv b \ (mod. m)$. Daí $ax_1 \equiv b \ (mod. m)$.

Assim, se conhecemos uma solução x_0 da congruência $ax \equiv b \ (mod. m)$, então conhecemos uma família de soluções da mesma, onde tal família é o conjunto:

$$\{y \in \mathbb{Z}; y \equiv x_0 \ (mod. m)\} = conjunto\ de\ resíduos\ de\ x_0\ módulo\ m.$$

Portanto, soluções diferentes para a congruência $ax \equiv b \ (mod. m)$ serão aquelas incongruentes módulo m. Os teoremas a seguir respondem, respectivamente, as seguintes perguntas:

(1) sob que condições a congruência linear $ax \equiv b \ (mod. m)$ admite soluções?

(2) no caso de existirem soluções, quantas soluções incongruentes existem?

Teorema 3.14 Sejam a, b, x e $m > 0$ inteiros. A congruência linear $ax \equiv b\ (mod. m)$ admite solução se, e somente se, o $mdc(a, m)$ divide b.

Teorema 3.15 Seja $d = mdc(a, m)$. No caso em que $d|b$, a congruência linear $ax \equiv b\ (mod. m)$ admite exatamente d soluções mutuamente incongruentes módulo m. Além disso, se x_0 é uma solução particular de $ax \equiv b\ (mod. m)$, então as d soluções incongruentes módulo m são obtidas pela fórmula $x_0 + k \cdot \frac{m}{d},\ k \in \mathbb{Z},\ 0 \leq k \leq d - 1$. Em particular, se $d = 1$, então a congruência $ax \equiv b\ (mod. m)$ admite uma única solução módulo m.

Tais teoremas não serão demonstrados aqui, mas o leitor pode facilmente encontrar essas demonstrações em Santos (2014) ou Alencar Filho (1989).

Exemplo 3.17 Vamos resolver as congruências $18x \equiv 30\ (mod. 42)$ e $4x \equiv 8\ (mod. 15)$. Note inicialmente que $mdc(18, 42) = 6$. Logo, como $6|30$, segue do Teorema 3.15 que a congruência $18x \equiv 30\ (mod. 42)$ admite exatamente 6 soluções mutuamente incongruentes módulo 42.

Por tentativas, encontramos $x_0 = 4$ como solução particular de $18x \equiv 30\ (mod. 42)$, uma vez que $18 \cdot 4 = 72 = 42 \cdot 1 + 30$. Portanto, como assegurado no Teorema 3.15, as 6 soluções incongruentes da congruência $18x \equiv 30\ (mod. 42)$ serão dadas pela fórmula $4 + k \cdot \frac{42}{6} = 4 + 7k$, com $0 \leq k \leq 5$. São elas:

$$\underbrace{4 + 7 \cdot 0}_{=4}; \underbrace{4 + 7 \cdot 1}_{=11}; \underbrace{4 + 7 \cdot 2}_{=18}; \underbrace{4 + 7 \cdot 3}_{=25}; \underbrace{4 + 7 \cdot 4}_{=32}.$$

Portanto, as soluções da congruência $18x \equiv 30\ (mod. 42)$ são os inteiros: 4, 11, 18, 25, 32 e 39.

Com relação à congruência $4x \equiv 8\ (mod. 15)$, como $mdc(4, 15) = 1$, segue que a mesma admite uma única solução módulo 15. Como já é nítido, $x_0 = 2$ é uma solução particular. Portanto, essa é a única solução incongruente módulo 15 da congruência dada. Isso significa que qualquer outra solução x da congruência $4x \equiv 8\ (mod. 15)$ é tal que $x \equiv 2\ (mod. 15)$. Dizemos então que $x \equiv 2\ (mod. 15)$ é a solução geral da congruência $4x \equiv 8\ (mod. 15)$.

Na próxima seção passaremos a estudar um pouco do método RSA, sua funcionalidade e como o mesmo está relacionado com alguns métodos de teoria dos números que estudamos nesta seção.

3.2 O método criptográfico RSA

De acordo com Sautoy (2007), um artigo de uma dupla de matemáticos da universidade de Stanford – Whit Diffie e Martin Hellman – chamado *novos caminhos da criptografia*, teria sido o primeiro a propor a criptografia de chave pública no meio científico. Até então, todos os métodos criptográficos existentes eram de chave privada. Todavia, mesmo com a ideia desse novo tipo de criptografia, o artigo de Diffie e Hellman não dava nenhuma garantia que tal criptografia pudesse realmente existir, isto é, se seria possível desenvolver um método criptográfico que possuísse as propriedades de um sistema de criptografia de chave pública.

Felizmente, não só foi possível desenvolver um método desse tipo, como também fixá-lo fortemente em conceitos e resultados da teoria dos números. O primeiro método proposto de criptografia de chave pública foi desenvolvido por um trio de cientistas do Instituto de Tecnologia de Massachusetts (MIT) – Ron Rivest, Adi Shamir e Leonard Adleman – em 1978. Este método foi nomeado de RSA em alusão as iniciais dos sobrenomes de seus inventores. O RSA é um dos métodos de criptografia de chave pública mais importante e seguro do mundo, usado principalmente em aplicações comerciais via internet. "Este é o método utilizado, por exemplo, no Netscape, o mais popular dos Softwares de navegação da internet" (COUTINHO, 2005, p. 3).

Como sabemos, os métodos de criptografia de chave pública atuam com duas chaves, uma pública e outra privada. No RSA, a chave pública constitui-se de um número natural N, o qual é originado a partir da multiplicação de dois números primos p e q ($ímpares$), isto é, $N = p.q$. Para codificar uma mensagem M usamos N, e para decodificá-la usamos os fatores primos p e q que geraram N. Portanto, N é a chave pública e o par p, q a chave privada. A rigor, tais chaves ainda vão requerer outros inteiros positivos, que destacaremos mais adiante.

Como a chave privada é p e q, logo entendemos que é muito fácil quebrar o código RSA, pois é só fatorar N, certo? Certo! Porém, fatorar N e descobrir seus fatores primos p e q pode se tornar uma tarefa muito difícil, mesmo para os melhores computadores. A fatoração de N é dificultada por dois motivos: primeiro porque os números primos utilizados nas chaves do RSA são gigantescos. Logo, o número N será enorme, com centenas de dígitos, dificultando muito sua fatoração. E segundo porque fatorar N em tempo útil ainda é um dos problemas mais complicados da matemática. A esse respeito, Coutinho (2005) reitera o que acabamos de mencionar:

> Usando como chaves de codificação do RSA números muito grandes (de 150 algarísmos ou mais), fatorar $\boldsymbol{N}$ para achar p e q, com os métodos atuais levaria alguns milhares de anos. É disto que depende a segurança do RSA; da ineficiência dos métodos de fatoração atualmente conhecidos. (COUTINHO, 2005, p. 4, **grifo nosso**)

Portanto, o problema da fatoração é o que garante ao RSA a segurança da sua chave privada. No entanto, é preciso frisar que não é impossível, para um intruso, descobrir a chave privada, pois apesar do problema da fatoração ser muito complicado para números muito grandes, isso não descarta a possibilidade de N ser fatorado num determinado tempo, mesmo que esse tempo seja consideravelmente longo.

Dessas considerações iniciais já temos uma boa ideia da segurança do RSA e no que ela se baseia apesar dessa segurança ser muito mais complexa do que parece. Todavia, podemos nos convencer da eficiência e privacidade do RSA e passar a explorar seus processos de codificação e decodificação. Portanto, passaremos a discutir agora sobre alguns aspectos desses processos, buscando entender como aquelas ideias de aritmética básica que abordamos estão relacionadas com o RSA.

3.2.1 O processo de pré-codificação no RSA

Antes de abordarmos a codificação e decodificação no RSA, é preciso destacar um processo preliminar, chamado de pré-codificação. Para realizar essa pré-codificação, estabelecemos algumas restrições, que só aparecem aqui com o intuito de simplificar nossa apresentação do RSA. Em trabalhos voltados para a criptografia, essas restrições não são feitas, com exceção da restrição (1) abaixo, pois se trabalha com o RSA de modo geral e num nível muito mais avançado. As restrições são as seguintes:

(1) Em geral, a mensagem será tratada como um texto, cujas palavras são formadas por letras de um alfabeto fixado. No nosso caso, o alfabeto a ser utilizado é o usual: A, B, C, ..., Z;

(2) A mensagem não pode conter números em seu conteúdo. Isso não quer dizer que o RSA não codifica números. Pelo contrário, há também um processo específico para a codificação de números. Veja, por exemplo, Buchmann (2002, p. 162);

(3) A mensagem original e a codificada serão dadas em letras maiúsculas e desconsideraremos os acentos das palavras. Apenas levamos em conta as letras que compõem as palavras e os espaços entre essas palavras. Os sinais de pontuação não serão levados em conta aqui.

Depois disso, estabelecemos uma tabela de conversão, onde associamos a cada letra do nosso alfabeto um número, que no nosso caso será de dois dígitos, como segue.

Tabela 7 – Tabela de conversão

A	B	C	D	E	F	G	H	I	J
11	12	13	14	15	16	17	18	19	20

K	L	M	N	O	P	Q	R	S	T
21	22	23	24	25	26	27	28	29	30

U	V	W	X	Y	Z
31	32	33	34	35	36

Fonte: autoria própria

Não utilizamos números de um dígito porque isso pode causar certas ambiguidades. Por exemplo, se o A fosse representado por 3, quem seria 33? Poderia ser AA ou W. Assim, é melhor utilizarmos números com dois dígitos. Do mesmo modo, essa associação é aleatória e não sequencial, porém tomando o cuidado evidenciado anteriormente. Para os espaços entre as palavras utilizamos o número 99. Assim, cada mensagem será transformada em uma sequência de dígitos. Por exemplo, a mensagem A ARTE DOS CÓDIGOS SECRETOS será convertida, de acordo com a Tabela 7, na seguinte sequência de dígitos:

11991128301599142529991325141917252999291513281530 2529

3.2.2 O processo de codificação no RSA

Depois que já convertemos a mensagem em uma sequência de dígitos, o próximo passo é escolher os *parâmetros* de codificação e decodificação, que são dois números primos p e q (de preferência da mesma ordem de grandeza[30]), cujo produto resulta em N. A sequência é então subdividida em blocos, onde cada um desses blocos são números inteiros positivos menores do que N. Segundo Coutinho (2009, p. 148) apud Medeiros (2017, p. 47):

[30] A ordem de grandeza de um número n é a potência de 10 mais próxima desse número.

> A maneira de escolher os blocos não é única e os blocos não precisam sequer ter o mesmo tamanho. Contudo, certos cuidados devem ser tomados. Por exemplo, não é permitido escolher um bloco que comece por 0 porque isto traria problemas na hora de decodificar, já que, por exemplo, não temos como distinguir o bloco 071 do bloco 71.

Sendo assim, depois de convertermos a sequência de dígitos em blocos, tomando os devidos cuidados, podemos seguir na codificação da mensagem. Considere, então, que b seja um bloco qualquer da mensagem pré codificada. Para codificarmos a mensagem, devemos codificar todos os blocos obtidos. A questão é: como devemos realizar a codificação de cada um desses blocos? Para realizar essa codificação, primeiro devemos considerar o inteiro positivo $N = p.q$, onde já sabemos que p e q são números primos. Segundo, introduziremos uma nova variável e, tal que, e é relativamente primo com $\varphi(N) = (p-1)(q-1)$, isto é, $mdc\big(e, \varphi(N)\big) = 1$.

Especificamente, o que chamamos de chave pública do RSA é o par (N, e), o qual será utilizado para codificar cada bloco b. Denotemos por $C(b)$ o bloco b codificado. Para obter $C(b)$, consideremos a seguinte congruência:

$$c(b) \equiv b^e (mod. N)$$

Ou seja, $c(b)$ e b^e deixam o mesmo resto na divisão por N. Por convenção, $c(b)$ deve ser um inteiro positivo menor do que N. Daí, se b^e deixa resto r na divisão por N, segue que $C(b) \equiv\ b^e \equiv r(mod. N)$, $0 \leq r < N \Longrightarrow C(b) = r$. Conclusão:

$$C(b) = resto\ da\ divisão\ de\ b^e\ por\ N.$$

A seguir, temos o resumo dos processos de codificação e decodificação no algoritmo RSA.

Algoritmo 3.1 – Processo de codificação utilizando o RSA

Codificação
ENTRADA: mensagem **M**
Etapa 1: **M** é pré codificada com base em uma tabela (como a Tabela 7), onde cada letra e espaço entre palavras é substituído por um número. **Etapa 2**: Escolhem-se dois números primos grandes $\boldsymbol{p}$ e $\boldsymbol{q}$ (da mesma ordem de grandeza, de preferência) e efetua-se a multiplicação entre eles dando origem a um número $\boldsymbol{N = p \cdot q}$. **Etapa 3**: A mensagem **M** pré codificada é dividida em blocos (números) menores do que $\boldsymbol{N}$.

Etapa 4: Escolhe-se um inteiro positivo $\boldsymbol{e}$, com $\boldsymbol{e} < (p-1)(q-1) = \varphi(N)$ e tal que $\boldsymbol{e}$ seja relativamente primo com $\varphi(N)$, isto é, $mdc\big(e, \varphi(N)\big) = 1$. O par $\boldsymbol{(e, N)}$ é a chave de codificação. **Etapa 5**: Cada bloco $\boldsymbol{b}$ que compõe a mensagem pré codificada será codificado segundo a regra: $$\boldsymbol{C(b) = resto\ da\ divisão\ de\ b^e\ por\ N}.$$ Onde $\boldsymbol{C(b)}$ representará o bloco b codificado. A mensagem codificada será então a sequência formada por todos os blocos codificados, respeitando a ordem em que os mesmos aparecem na mensagem original M.
SAÍDA: a mensagem codificada $\boldsymbol{M'}$

Fonte: Autoria própria

Exemplo 3.18 Vamos codificar a palavra UFERSA seguindo o Algoritmo 3.1.

Entrada: UFERSA

Etapa 1: De acordo com a Tabela 7, a palavra UFERSA será convertida na seguinte sequência de dígitos:

311615282911

Etapa 2: Nossos parâmetros serão os primos $p = 17$ e $q = 31$. É claro que poderia ser quaisquer dois primos distintos p e q ímpares, mas para simplificar os cálculos, escolhemos primos pequenos. Assim, $N = 17 \cdot 31 = 527$.

Etapa 3: Devemos quebrar a sequência de dígitos 311615282911 em blocos c, onde c é um número inteiro positivo menor que 527. Uma possibilidade para essa divisão em blocos é:

31-161-52-82-9-11.

Etapa 4: Por fim, precisamos determinar um natural e, tal que, $mdc\big(e, \varphi(527)\big) = 1$. Ora, como a função φ é multiplicativa e $527 = 17 \cdot 31$, com 17 e 31 números primos, segue que $\varphi(527) = \varphi(17 \cdot 31) = \varphi(17) \cdot \varphi(31) = 16 \cdot 30 = 480$. Tomando $e = 7$, temos que o $mdc\big(7, \varphi(527)\big) = mdc(7, 480) = 1$. Portanto, a chave de codificação (chave pública) será o par $(7, 527)$.

Etapa 5: Agora, codificaremos cada um dos blocos 31,161,52,82,9,11 usando a regra $C(b) = resto\ da\ divisão\ de\ b^e\ por\ N$. A mensagem codificada será a sequência de blocos codificados, também separados, obtidos nesse processo. Sendo assim, teremos:

Codificação do bloco 31

Neste caso, $b = 31$, logo $C(31) =$ *resto da divisão de* 31^7 *por 527*.
Como $31^3 \equiv 279\ (mod. 527)$, através das propriedades vistas no Teorema 3.8 temos que $31^6 \equiv 279^2 \equiv 372\ (mod. 527) \Longrightarrow 31^7 \equiv 31.372 \equiv 465\ (mod. 527)$.
Portanto, consideraremos $C(31) = 465$, que é o resto da divisão de 31^7 *por 527*. Assim, dizemos que o bloco 31 depois de codificado passará a ser o bloco 465.
De modo inteiramente análogo, podemos codificar os demais blocos. Não realizaremos os cálculos detalhadamente, mas isso não apresenta grandes dificuldades porque os números são pequenos.

Codificação do bloco 161

$C(161) =$ *resto da divisão de* 161^7 *por 527*. Como $161^2 \equiv 98\ (mod. 527)$, temos que $161^6 \equiv 98^3\ (mod. 527) \Longrightarrow 161^6 \equiv 497 (mod. 527) \Longrightarrow 161^7 \equiv 161.497 (mod. 527) \Longrightarrow 161^7 \equiv 440 (mod. 527)$. Logo, teremos $C(161) = 440$ e o bloco 161 passará a ser 440.

Codificação do bloco 52

Analogamente, $C(52) \equiv 52^7\ (mod. 527)$. Precisamos determinar o resto da divisão de 52^7 por 527. Calculando $52^3 = 140608$ e dividindo por 527, obtemos como resto dessa divisão o número 426. Logo, teremos $52^3 \equiv 426\ (mod. 527) \Longrightarrow 52^6 \equiv 426^2\ (mod. 527) \Longrightarrow 52^6 \equiv 188\ (mod. 527)$. Portanto, $52^7 \equiv 52.188\ (mod. 527) \Longrightarrow 52^7 \equiv 290\ (mod. 527)$. Logo, $C(52) = 290$.

Codificação do bloco 82
Temos: $C(82) \equiv 82^7\ (mod. 527)$. Fazendo as contas, temos $82^3 \equiv 126(mod. 527)$. Logo, $82^6 \equiv 126^2 \equiv 66(mod. 527) \Longrightarrow 82^7 \equiv 82.66 \equiv 142(mod. 527)$. Portanto, $C(82) = 142$.

Codificação do bloco 9
Como uma calculadora, calculamos o valor de 9^7, obtendo $9^7 = 4782969$. Dividindo esse número por 527, obtemos resto igual a 444. Portanto, $9^7 \equiv 444(mod. 527)$, donde $C(9) = 444$.

Codificação do bloco 11
Neste caso, temos $11^4 = 14641 = 527 \cdot 27 + 412$ e $11^3 = 1331 = 527 \cdot 2 + 277$. Logo, $11^4 \equiv 412(mod. 527)$ e $11^3 \equiv 277(mod. 527)$. Multiplicando essas duas últimas congruências, obtemos $11^7 \equiv 412 \cdot 277 \equiv 292(mod. 527)$. Portanto, $C(11) = 292$.

Saída: 465-440-290-142-444-292.

Relembrando que os blocos codificados devem permanecer separados. Por outro lado, se quisermos reverter o processo e decodificar a palavra UFERSA, deveremos seguir um novo processo, que descreveremos a seguir.

3.2.3 O processo de decodificação no RSA

Nesta seção iremos analisar o processo de decodificação no RSA. Para realizarmos esse processo, ainda é necessário o conhecimento do inteiro $N = p \cdot q$. No entanto, outro número inteiro será incluído. Esse número será denotado por d e escolhido de tal modo que ele seja o inverso multiplicativo de e módulo $\varphi(N)$ (aqui já percebemos a dificuldade de

quebrar o RSA, pois para calcular d precisamos de $\varphi(N)$, mas o valor de $\varphi(N)$ é difícil de calcular porque os fatores primos $p\ e\ q$ não são de conhecimento do público). Lembre-se que e juntamente com N formam a chave pública do sistema RSA. Como vimos, o fato de d ser o inverso multiplicativo de e módulo $\varphi(N)$ significa que $d \cdot e \equiv 1(mod.\varphi(N))$. Como e foi escolhido de modo a ser relativamente primo com $\varphi(N)$, segue que sempre existirá o inverso multiplicativo de e módulo $\varphi(N)$, donde a existência de d está garantida.

Portanto, se $C(b)$ denota o bloco b codificado, então $D(C(b))$ indicará o bloco $C(b)$ decodificado. Isto significa que recuperamos o bloco b. Ou seja, que $D\big(C(b)\big) = b$. Para calcular $D(C(b))$ usaremos uma receita parecida com a de calcular $C(b)$. Temos que,

$$D\big(C(b)\big) = resto\ da\ divisão\ de\ C(b)^d\ por\ N.$$

Em termos de congruências, temos que:

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

O par (N, d) será chamado de chave secreta (privada) do sistema RSA e sua posse é de uso restrito. É com essa chave que podemos decodificar todas as mensagens codificadas com a chave (N, e). Naturalmente, para decodificar a mensagem por inteira devemos decodificar cada um dos blocos codificados.

O Algoritmo 3.2 a seguir resume as etapas do processo de decodificação no RSA.

Algoritmo 3.2 – Processo de decodificação usando o RSA

Decodificação
Entrada: uma mensagem codificada M'
Etapa 1: Calcula-se o inverso multiplicativo de e módulo $\varphi(N)$, isto é, calcula-se um inteiro positivo $\boldsymbol{d}$, $1 < \boldsymbol{d} < \varphi(N)$, tal que $\boldsymbol{d \cdot e \equiv 1(mod.\varphi(N))}$. **Etapa 2**: Cada bloco $C(b)$ será decodificado segundo a regra: $$\boldsymbol{D\big(C(b)\big) = resto\ da\ divisão\ de\ \big(C(b)\big)^d\ por\ N}$$ Isto equivale a dizer que $D\big(C(b)\big) \equiv \big(C(b)\big)^d (mod.N)$. Ou seja, $b \equiv \big(C(b)\big)^d (mod.N)$. O bloco b será então igual ao resto da divisão de $\big(C(b)\big)^d$ por N.
Saída: A mensagem original M

Fonte: Autoria própria

Exemplo 3.19 Por meio do Algoritmo 3.2 já sabemos como decodificar mensagens no RSA. Nos preocuparemos, agora, em recuperar a mensagem 465-440-290-142-444-292 codificada no Exemplo 3.18. Devemos decodificar cada um dos blocos e, portanto, decodificar a mensagem por inteira seguindo as etapas dadas no Algoritmo 3.2.

Etapa 1: A chave pública que utilizamos foi $(7, 527)$. Para calcular o valor de d, devemos resolver a congruência $7d \equiv 1(mod.\varphi(527))$. Como já temos os fatores primos que geraram 527, fica fácil calcular $\varphi(527)$ (como sabemos, na prática isso não acontece, pois os fatores p e q não são publicados). Temos $\varphi(527) = \varphi(17 \cdot 31) = 480$. Logo, $7d \equiv 1(mod.480)$. Como o módulo dessa última congruência é um número grande, tentar encontrar d por tentativas fica muito difícil. Sendo assim, o que geralmente é feito é transformar a congruência $7d \equiv 1(mod.480)$ numa equação do tipo $ax + by = c$, com a, b, c, x e y inteiros[31]. Ora, se $7d \equiv 1(mod.480)$, então existe $k \in \mathbb{Z}$, tal que $7d = 480k + 1$, o que implica $7d - 480k = 1$, que é uma equação diofantina. Resolvendo essa equação, obtemos uma solução $(343, 5)$. Logo, uma solução para $7d \equiv 1(mod.480)$ é $d = 343$. Assim sendo, a chave secreta será $(527, 343)$.

Etapa 2: Passemos às decodificações. Como os cálculos agora serão mais trabalhosos e extensos, pois os números serão muito grandes, optaremos por descrever aqui apenas alguns passos do cálculo do bloco $D(465)$. Para os demais daremos apenas o resultado final, deixando a tarefa de verificar as contas por parte do leitor.

Decodificação do bloco 465

Devemos calcular o resto da divisão de 465^{343} por $N = 527$ para obter $D(465)$. Começamos calculando $465^3 = 100544625$. O resto da divisão desse número por 527 é 403, donde $465^3 \equiv 403(mod.527)$. A partir daí, temos as implicações seguintes, que o leitor pode verificar sem problema algum:

$$465^3 \equiv 403(mod.527) \Longrightarrow 465^6 \equiv 93(mod.527) \Longrightarrow 465^{12} \equiv 217(mod.527).$$

Agora, como $343 = 28.12 + 7$, elevamos os dois lados da congruência $465^{12} \equiv 217(mod.527)$ a 28, obtendo $465^{336} \equiv 217^{28}(mod.527)$. Precisamos determinar o resto da divisão do número 217^{28} por 527. Com mais alguns cálculos, que podem ser

[31] Essas equações são chamadas de equações diofantinas (em homenagem ao matemático Diofanto de Alexandria). Para estudar os métodos de resolução dessas equações, o leitor pode consultar Santos (2014) ou Alencar Filho (1989).

rápidos se tivermos um computador por perto, podemos calcular este resto facilmente. Teremos:

$$217^3 \equiv 310(mod.527) \Longrightarrow 217^6 \equiv 186(mod.527) \Longrightarrow 217^{12} \equiv 341(mod.527)$$
$$\Longrightarrow 217^{24} \equiv 341(mod.527)$$
$$\Longrightarrow 217^{28} = 217^{24}.217^4 = 217^{24}.217^3 217 \equiv 341.310.217(mod.527)$$

Como $341.310.217 = 22939070 = 43527.527 + 341$, segue que

$$217^{28} \equiv 341.310.217 \equiv 341(mod.527).$$

Portanto, $465^{336} \equiv 217^{28} \equiv 341(mod.527)$. Para finalizar, multiplicamos os dois lados desta última congruência por 465^7, considerando que $465^7 \equiv 31(mod.527)$. Teremos, então

$$465^7.465^{336} \equiv 465^7.341(mod.527) \Longrightarrow 465^{343} \equiv 31.341 \equiv 31(mod.527).$$

Portanto, o resto da divisão de 465^{343} por 527 é 31, isto é, $D(465) = D\big(C(31)\big) = 31$ e recuperamos o bloco 31.

Utilizando um raciocínio análogo ao anterior, podemos recuperar os demais blocos. A tabela a seguir apresenta os demais resultados da decodificação.

Decodificação dos demais blocos:
$D(440) = D\big(C(161)\big) = 161$
$D(290) = D\big(C(52)\big) = 52$
$D(142) = D\big(C(82)\big) = 82$
$D(444) = D\big(C(9)\big) = 9$
$D(292) = D\big(C(11)\big) = 11$

Saída: 31-161-52-82-9-11

Terminado esse processo de decodificação, obteremos a seguinte sequência de blocos: 31-161-52-82-9-11, que corresponde a palavra UFERSA de acordo com a Tabela 7.

É claro que os cálculos anteriores são muito complicados para serem feitos com lápis e papel. Na prática pode-se utilizar uma calculadora profissional, um aplicativo de celular ou um programa de computador para efetuar essas divisões com números muito grandes. Evidentemente, nas aplicações do RSA no mundo real, todos os cálculos são feitos por

computador. O leitor pode desenvolver novos exemplos com números menores para facilitar o entendimento dos processos de codificação e decodificação. O importante, com base no propósito deste trabalho, é entender como os conceitos de aritmética se manifestam nesse sistema criptográfico. Isto trará um entendimento mais sólido sobre o funcionamento do RSA e facilitará uma possível exposição desse método como uma aplicação da teoria dos números, em particular da aritmética básica, em sala de aula.

Assim sendo, para auxiliar o professor, caso o mesmo deseje trabalhar o RSA como aplicação da aritmética básica em suas aulas, os Exemplos 3.18 e 3.19, com o auxílio dos Algoritmos 3.1 e 3.2, foram desenvolvidos de modo a explicitar uma possível sequência didática que facilite a aplicação desse método criptográfico em sala de aula. De modo simples e fácil, o professor pode utilizar o passo a passo dado nos algoritmos para explicar como funcionam os processos de codificação e decodificação no RSA. Consequentemente, esse passo a passo pode ser utilizado na resolução de problemas envolvendo codificação e decodificação de mensagens por meio do RSA como foi feito nos Exemplos 3.18 e 3.19. Isto torna muito mais fácil a aplicação e entendimento do RSA, bem como a compreensão da matemática envolvida. Além de apresentar ao aluno situações práticas e reais em que a matemática está diretamente envolvida.

Para finalizarmos este capítulo, explicaremos brevemente porque o RSA funciona e em que se baseia sua segurança com base no que vimos sobre aritmética básica. Inicialmente, como estamos tratando de um método de criptografia, os processos de codificação e decodificação associados a ele devem ser bem específicos e relacionados de tal modo que sempre deverá ser possível recuperar um bloco codificado, isto é, reverter o processo de codificação. No caso do RSA, é possível provar que $D\big(C(b)\big) = b$ qualquer que seja o bloco b. Uma demonstração desse resultado pode ser encontrada em Coutinho (2005, p. 184). Isso garante que sempre que decodificarmos um bloco codificado voltaremos ao bloco b. De modo geral, sempre que decodificarmos um texto codificado, voltaremos ao texto original.

Quanto à segurança do RSA, a mesma está apoiada na dificuldade de fatorar o inteiro N, como já citado. Sendo (N, e) a chave pública do sistema, para quebrá-lo seria preciso fatorar N e descobrir os fatores primos p e q. Conhecido os fatores primos, conhecemos $\varphi(N)$ e, consequentemente, descobrimos d que é a chave privada propriamente dita, uma vez que $d \cdot e \equiv 1(mod.\varphi(N))$ e e é público. No entanto, é muito difícil fatorar N em tempo útil, pois como já citamos, os primos utilizados no RSA podem ter mais de 300 algarismos, de modo

que poderia levar centenas de anos para que certas fatorações pudessem ser realizadas com os métodos que hoje existem. No entanto, se é muito complicado fatorar N, então o método RSA está livre de ataques? Ou melhor, existem outros modos para tentar vencer este sistema? Bom, há vários fatores que poderiam influenciar na quebra desse sistema, mas isso só é tratado em livros especializados em criptografia. Uma dessas maneiras está ligada a escolha dos primos que darão origem ao inteiro N. Se eles forem mal escolhidos, isso pode acarretar em facilidade para fatorar N. Outra maneira que poderia tornar o RSA obsoleto seria a invenção de um algoritmo de fatoração de tempo polinomial, isto é, que conseguisse fatorar qualquer número inteiro muito rapidamente. Até agora tal algoritmo não existe, mas não se descarta a possibilidade de um dia um vir a ser inventado.

O que também poderia dar certo para vencer o RSA seria conseguir determinar d sem ter que fatorar N. Ou então obter $\varphi(N)$ sem conhecer p e q. No entanto, esses são problemas para os quais uma solução ainda não existe, o que é muito bom para a segurança do RSA. Enfim, enquanto não existir uma maneira rápida para fatorar inteiros ou um método para calcular d sem recorrer à fatoração, o RSA permanecerá intacto e nossas senhas de cartões de créditos e transações comerciais via internet estarão seguros. Logicamente, a segurança do RSA é muito mais delicada do que possa parecer, e muitos outros fatores podem influenciar nessa segurança. Para o leitor interessado em aprofundar seus estudos em criptografia, em especial a criptografia RSA, as obras já citadas constituem uma rica fonte de informações sobre o assunto.

4 APLICAÇÕES II: ALGUNS CONCEITOS DE MATEMÁTICA BÁSICA EM CRIPTOGRAFIA

Destacamos mais uma vez o objetivo central deste trabalho que é investigar a relação entre matemática básica e criptografia e como essa relação pode nos render ferramentas para a melhoria do ensino e aprendizagem de matemática. No Capítulo 2 já citamos elementos simples de matemática que tem relação com criptografia, como análise combinatória, por exemplo. No Capítulo 3 nosso objetivo foi ressaltar que a aritmética básica também está inserida na ciência dos códigos. Para finalizar nossa investigação, trataremos neste capítulo de revisar alguns temas de matemática do ensino médio e relacioná-los com algum método de criptografia. Essa relação, na maioria das vezes dada por meio de exemplos, funcionará como uma aplicação daquele assunto na criptografia e como ferramenta principal de motivação para o desenvolvimento de atividades em sala de aula. Este capítulo fundamenta-se em obras, tais como: Buchmann (2002), Lima *et al*. (2006a), Lima (2013), Lima *et al*. (2006b), França (2014), Tavares et al. (2017), entre outros.

4.1 Conjuntos, Funções e Criptografia

Conjuntos e funções são tópicos já consagrados de matemática no ensino básico. Seu estudo é indispensável para a compreensão e o desenvolvimento de toda a matemática. Como consequência disso, o conhecimento nessa área nos dá condições de compreender mais detalhadamente como funciona e se estrutura a matemática da criptografia. Sendo assim, nesta seção desenvolveremos um pouco da teoria relacionada com conjuntos e funções. Como nosso estudo frisa a matemática básica, não nos estenderemos nessas teorias. Apresentaremos alguns conceitos básicos, porém necessários, para melhor proveito e compreensão de como os mesmos se fazem presentes na criptografia. Começaremos revisando alguns fatos básicos sobre a *Linguagem de Conjuntos*.

4.1.1 Noções básicas sobre Conjuntos

"Toda a matemática atual é formulada na linguagem de conjuntos. Portanto, a noção de conjunto é a mais fundamental: a partir dela, todos os conceitos matemáticos podem ser expressos" (LIMA et al., 2006a, p. 1). A importância do conceito de conjunto, destacado

anteriormente, também é notória em criptografia. Como veremos ao longo deste capítulo, os conjuntos aparecerão como simplificadores de notações, bem como simplificadores da linguagem utilizada para descrever o funcionamento dos métodos criptográficos em geral. Portanto, é de suma importância o conhecimento de noções básicas de conjuntos, tais como notação, quantidade de elementos e operações.

Para isso, precisamos entender inicialmente o que é um conjunto. Na realidade, não há uma definição precisa para conjuntos com base em outros conceitos já definidos. Ou seja, a noção de conjunto é primitiva. Isso significa que ela será adotada sem definição, aceita como algo conhecido por todos. Assim como na geometria, onde adotamos os conceitos de ponto, reta e plano como primitivos, e a partir daí desenvolvemos toda a teoria, nas exposições sobre *linguagem de conjuntos* também seguimos esse mesmo raciocínio: aceitamos o conceito de conjunto sem definição, e a partir daí nos preocupamos em saber como são constituídos os conjuntos, como se relacionam e quais as suas propriedades. Assim, segundo Lima *et al*. (2006a, p.1):

> Um conjunto é formado por elementos. Dados um conjunto A e um objeto qualquer a (que pode até mesmo ser outro conjunto), a única pergunta cabível em relação a eles é: a é ou não um elemento do conjunto A? No caso afirmativo, diz-se que a pertence ao conjunto A e escreve-se $a \in A$. Caso contrário, põe-se $a \notin A$ e diz-se que a não pertence ao conjunto A. (LIMA et al., 2006a, p. 1)

A relação *a pertence ao conjunto A* é dita relação de *pertinência*. Como de costume, utilizamos letras latinas maiúsculas para indicar os conjuntos, e letras latinas minúsculas para indicar os seus elementos. A representação formal de um conjunto será, portanto, a seguinte:

$$A = \{a, b, c, d, e, \dots\}.$$

Podemos destacar muitos conjuntos importantes: os conjuntos numéricos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ (além do conjunto $\mathbb{C}$ dos números complexos), conjuntos de pontos e de retas na geometria, conjunto de figuras geométricas (triângulos, quadriláteros, *etc*), conjuntos de funções, matrizes, entre muitos outros. Além desses, podemos destacar o conjunto que não contém nenhum elemento, chamado conjunto vazio e indicado pelo símbolo $\emptyset$, e os conjuntos unitários que são aqueles que possuem um único elemento. Na criptografia, na área de computação, o conjunto (que mais tarde iremos chamar de alfabeto) $\{0, 1\}$ é essencial para a linguagem binária, base do sistema computacional moderno.

Definição 4.1 Sejam A e B conjuntos. Se para cada elemento $x \in A$ for verdade que $x \in B$ (ou seja, se todo elemento de A for também elemento de B), então diremos que o conjunto A está contido no conjunto B. Indicamos isto com a notação $A \subset B$. Neste caso, dizemos também que A é um subconjunto de B, ou que A é uma parte de B. Por outro lado, se existir ao menos um elemento $x \in A$ tal que $x \notin B$, dizemos que A não está contido em B, ou que A não é um subconjunto de B, ou que A não é uma parte de B e denotamos por $A \not\subset B$.

Exemplo 4.1 O conjunto $\mathbb{N}$ dos números naturais está contido no conjunto $\mathbb{Z}$ dos números inteiros, pois todo número natural também é inteiro. No geral, temos $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Exemplo 4.2 Seja $\mathcal{P}$ o conjunto dos números primos e B o conjunto dos números da forma $F_n = 2^{2^n} + 1$ (n inteiro não negativo), chamados números de Fermat[32]. Fermat chegou a conjecturar que todo número da forma $2^{2^n} + 1$ é primo, o que ele verificou ser verdade para os números F_0, F_1, F_2, F_3 e F_4. Euler[33] provou, anos depois, que a conjectura de Fermat era falsa. Euler conseguiu mostrar que o número F_5 é composto. Portanto, $B \not\subset \mathcal{P}$. Hoje sabemos que todos os números de Fermat conhecidos são compostos, exceto aqueles encontrados pelo próprio Fermat. Não se sabe se existem outros números primos de Fermat, veja Martinez *et al*. (2013).

A relação *A contido em B* é conhecida como relação de *inclusão*. Ela possui, qualquer que sejam os conjuntos A, B e C, as seguintes propriedades:

(i) $A \subset A$ para todo conjunto A. (*Propriedade reflexiva*);

(ii) se $A \subset B$ e $B \subset A$, então $A = B$. (*Propriedade anti - simétrica*);

(iii) se $A \subset B$ e $B \subset C$, então $A \subset C$. (*Propriedade transitiva*);

(iv) $\emptyset \subset A$

A Propriedade (ii) estabelece a *Igualdade de Conjuntos*. Ela assegura que dois conjuntos A e B são iguais se, e somente se, $A \subset B$ e $B \subset A$, isto é, se, e somente se, A e B possuem os mesmos elementos (LIMA et al., 2006a). Para indicar que A não é igual a B usamos a simbologia $A \neq B$. Neste caso, temos que $A \not\subset B$ ou $B \not\subset A$. Quando $A \subset B$, sendo

[32] Pierre de Fermat (1601 - 1665), matemático francês.
[33] Leonard Euler (1707 - 1783), matemático e físico suíço.

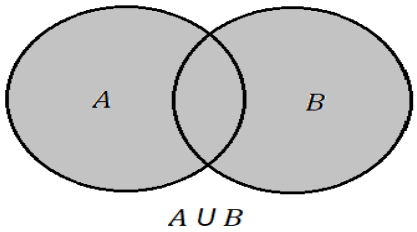
que $A \neq B$ e $A \neq \emptyset$, dizemos que A é uma parte própria de B, ou que A é um subconjunto próprio de B. Os subconjuntos A e $\emptyset$ de A são chamados de subconjuntos triviais.

Dado um conjunto A, o conjunto de todas as partes de A será indicado por $P(A)$. Ou seja, $P(A) = \{X; X \subset A\}$. Neste caso, dizer que $X \in P(A)$ é o mesmo que dizer $X \subset A$. Por exemplo, se $A = \{a, b, c\}$, então $P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. É possível provar, e já é bem conhecido que se A tem n elementos, então A possui 2^n subconjuntos, isto é, $P(A)$ tem 2^n elementos.

Definição 4.2 (*União de conjuntos*) Sejam dados dois conjuntos quaisquer A e B. Chama-se reunião, ou união, de A e B o conjunto formado por todos os elementos que pertencem a A ou a B. Denotaremos por $A \cup B = \{x; x \in A \; ou \; x \in B\}$.

Ou seja, para um elemento x pertencer a $A \cup B$ é necessário e suficiente que ele pertença a pelo menos um dos conjuntos A ou B.

Figura 10 – União de dois conjuntos



Fonte: Autoria própria

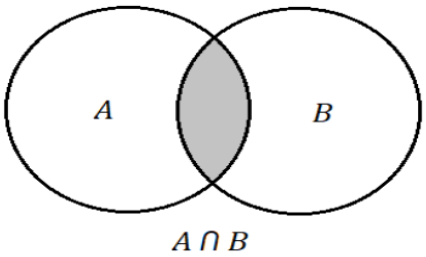
Na Figura 10 temos que os conjuntos A e B estão representados por círculos. A união de A com B é representada pela região cinza.

Exemplo 4.3 Se $A = \{1, 2, 3\}$ e $B = \{0, 4, 8, 10\}$, então $A \cup B = \{0, 1, 2, 3, 4, 8, 10\}$. Temos sempre que $A \subset A \cup B$ e $B \subset A \cup B$. Se $A \subset B$, então $A \cup B = B$. Para todo conjunto A, tem-se que $A \cup \emptyset = A$. Outras propriedades sobre a união de conjuntos podem ser encontradas em Alencar Filho (1972).

Definição 4.3 (*Intersecção de Conjuntos***)** Sejam dados dois conjuntos quaisquer A e B. Chama-se intersecção de A e B o conjunto formado por todos os elementos que pertencem a A e B simultaneamente. Denotaremos por $A \cap B = \{x; x \in A \text{ e } x \in B\}$.

Ou seja, para um elemento x pertencer a $A \cap B$ é necessário e suficiente que ele pertença A e também a B. A Figura 11 a seguir ilustra a intersecção $A \cap B$ indicada pela parte cinza.

Figura 11 – Intersecção de dois Conjuntos

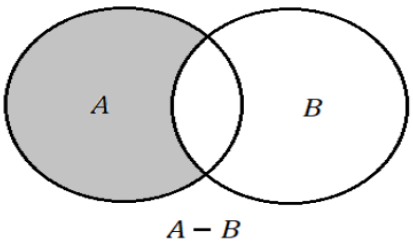


Fonte: Autoria própria

Exemplo 4.4 Se $A = \{1, 2, 3, 4, 5, 8, 10\}$ e $B = \{0, 4, 8, 10\}$, então $A \cap B = \{4, 8, 10\}$. Temos sempre que $A \cap B \subset A$ e $A \cap B \subset B$. Se $A \subset B$, então $A \cap B = A$. Para todo conjunto A, tem-se que $A \cap \emptyset = \emptyset$.

Definição 4.4 (*Diferença de conjuntos***)** Dados os conjuntos A e B, chama-se diferença entre A e B o conjunto formado por todos os elementos que pertencem à A, mas não pertencem à B. Denotaremos por $A - B = \{x; x \in A \text{ e } x \notin B\}$.

Figura 12 – Diferença de dois Conjuntos



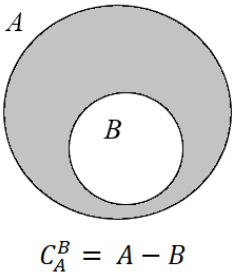
Fonte: Autoria própria

Exemplo 4.5 Se $A = \{1, 2, 3, 4, 5, 8, 10\}$ e $B = \{0, 4, 8, 10\}$, então $A - B = \{1, 2, 3, 5, \}$.

Quando $A \cap B = \emptyset$, nenhum elemento de A pertence à B, de modo que $A - B = A$ (LIMA, 2013). Na Figura 12 a diferença $A - B$ é indicada pela parte em cinza.

Definição 4.5 (*Complementar de um conjunto***)** Sejam A e B conjuntos quaisquer, tais que $B \subset A$. A diferença $A - B$ será dita o complementar de B com relação à A, e será indicada por C_A^B. Portanto, $C_A^B = A - B$.

Figura 13 – Complementar de B com relação à A



Fonte: Autoria própria

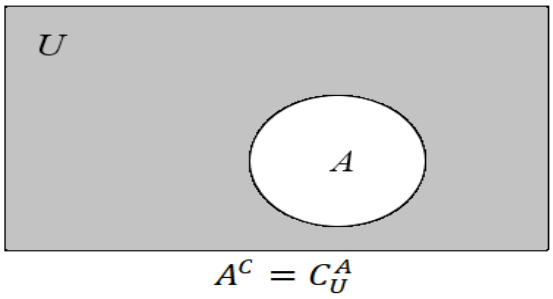
Exemplo 4.6 Seja $\mathbb{R}$ o conjunto dos números reais. A diferença $\mathbb{R} - \mathbb{Q}$ é o complementar de $\mathbb{Q}$ (conjunto dos números racionais) com relação à $\mathbb{R}$. O conjunto $\mathbb{R} - \mathbb{Q}$ é igual ao conjunto dos números irracionais.

Definição 4.6 (*Conjunto Universo*) Chama-se conjunto universo U o conjunto formado por todos os conjuntos tratados numa certa discussão (LIMA, 2013).

Isto quer dizer que quando considerarmos conjuntos A, B, C, ..., etc., existirá um conjunto maior que conterá todos esses conjuntos. Assim, por exemplo, quando abordamos a aritmética no Capítulo 3, nosso universo era o conjunto $\mathbb{Z}$ dos números inteiros (todos os conjuntos que tratamos eram subconjuntos de $\mathbb{Z}$).

Com a noção de conjunto universo definida podemos completar a definição de complementar de um conjunto. Assim, dado um conjunto A, contido num universo U, chama-se complementar de A com relação à U a diferença $U - A$, formada por todos os elementos de U que não pertencem a A. Em símbolos, temos $U - A = C_U^A = \{x \in U; x \notin A\}$. Para simplificar, usa-se apenas a notação A^C para indicar o complementar de A, sem fazer menção ao conjunto universo U: $A^C = C_U^A$.

Figura 14 – Complementar de A com relação ao Universo



Fonte: Autoria própria

Para finalizar essas considerações sobre conjuntos, abordaremos brevemente o importante conceito de conjunto finito.

Definição 4.7 Seja n um número natural. Com a notação I_n indicaremos o conjunto de todos os números naturais da sequência 1, 2, 3, ..., n. Isto é, $\mathrm{I}_n = \{1, 2, 3, \ldots, n\}$.

Exemplo 4.7 Para $n = 10$, tem-se $\mathrm{I}_{10} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Intuitivamente, um conjunto é finito quando podemos dizer quantos são os seus elementos, isto é, quando ele possui uma quantidade x de elementos. Para tornar essa noção mais rigorosa do ponto de vista matemático, precisamos tornar mais preciso o que se entende por uma contagem dos elementos de um conjunto, como veremos a seguir.

Definição 4.8 (*Conjuntos Finitos*) Um conjunto A é dito finito se for vazio (neste caso ele possui 0 elementos), ou então se existir um *função bijetiva* $f: \mathrm{I}_n \longrightarrow A$, do conjunto I_n no conjunto A. Neste último caso, dizemos que A tem n elementos.

A função bijetiva mencionada na definição anterior é a noção mais rigorosa de uma contagem dos elementos de A. Quando estabelecemos uma bijeção f de I_n em A, estamos contando os elementos de A. Para ficar mais clara essa contagem, consideremos que

$$f(1) = x_1, f(2) = x_2, \ldots, f(n) = x_n$$

Como f é uma função bijetiva, podemos garantir que todos os elementos de A foram contados (pois f é sobrejetiva), e somente uma única vez (pois f é injetiva). Logo, $A = \{x_1, x_2, \ldots, x_n\}$. Donde podemos contar os elementos de A.

Exemplo 4.8 O conjunto das letras do nosso alfabeto é finito e possui 26 elementos. O conjunto dos divisores de um número inteiro é finito. Se considerarmos o conjunto de todas as permutações da palavra criptografia, veremos que esse conjunto é finito e possui 59 875 200 elementos.

Quando um conjunto não é finito, ele será dito infinito. Portanto, um conjunto A é infinito quando não existe uma função bijetiva $f: \mathrm{I}_n \longrightarrow A$ qualquer que seja o n natural.

Exemplo 4.9 Os conjuntos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$ são todos infinitos. O conjunto dos números primos é infinito. O conjunto dos pontos do plano é infinito.

Na próxima seção estudaremos alguns tópicos relacionados ao conceito de função.

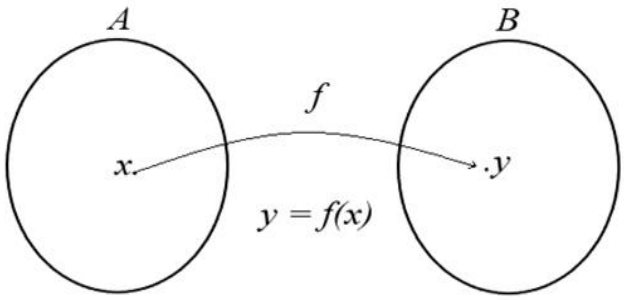
4.1.2 Noções básicas sobre Funções

De acordo com Lima (2013, p. 13),

> Uma função $f: A \to B$ consta de três partes: um conjunto A, chamado o domínio da função (ou o conjunto onde a função é definida), um conjunto B, chamado de contradomínio da função, ou o conjunto onde a função toma valores, e uma regra que permite associar, de modo bem determinado, a cada elemento $x \in A$, um único elemento $f(x) \in B$, chamado o valor que a função assume em x (ou no ponto x).

Assim, uma função nada mais é que uma receita (um algoritmo) que nos ensina como associar cada elemento de A a um único elemento de B. Quanto as notações, uma função f, de A em B, é comumente indicada por $f: A \to B$ (como já vimos anteriormente), ou $A \xrightarrow{f} B$, ou então $x \to f(x)$ para indicar que $f(x)$ é o valor associado à x por f. Dizemos que $y = f(x)$ é a imagem de x por f.

Figura 15 – Uma função f de A em B



Fonte: Autoria própria

Lima (2013) nos ensina ainda duas coisas importantes sobre funções:

1ª) Para todo $x \in A$, deve existir ao menos um $y \in B$, tal que, $y = f(x)$. Ou seja, a regra que ensina como obter $f(x)$ a partir de x deve valer para todos os elementos x do domínio de f;

2ª) Um elemento $x \in A$ só pode ter uma imagem $y = f(x) \in B$. Isto significa que se existir $x \in A$, tal que, $f(x) = y$ e $f(x) = y'$, então $y = y'$.

Exemplo 4.10 Fazendo $A = \mathbb{R}$ e $B = \mathbb{Z}$, podemos definir uma função $f: \mathbb{R} \to \mathbb{Z}$ pondo, para cada $x \in \mathbb{R}$, $f(x) = \lfloor x \rfloor = parte\ inteira\ de\ x$. Onde $\lfloor x \rfloor$ é o maior inteiro que não excede x.

Definição 4.9 Dizemos que duas funções f e g são iguais se elas possuírem o mesmo domínio, o mesmo contradomínio e a mesma lei de associação. Ou seja, dadas $f: A \to B$ e $g: C \to D$, $f = g \Leftrightarrow A = C, B = D$ e $f(x) = g(x)$ para todo $x \in A$.

Definição 4.10 Seja dada uma função $f: A \to B$. f é chamada de injetiva se dados x e x' em A, com $x \neq x'$, tivermos $f(x) \neq f(x')$ em B. Ou seja, uma função é injetiva quando elementos distintos no domínio possuem imagens distintas no contradomínio.

Exemplo 4.11 Toda função afim $f: \mathbb{R} \to \mathbb{R}$; $f(x) = ax + b$, com $a \neq 0$, é injetiva. Com efeito, dados x e x' em $\mathbb{R}$, com $x \neq x'$, temos:

$$ax \neq ax' \Longrightarrow ax + b \neq ax' + b \Longrightarrow f(x) \neq f(x').$$

Definição 4.11 Seja $f: A \to B$ uma função. Dizemos que f é sobrejetiva se para todo elemento $y \in B$ existe ao menos um $x \in A$ tal que $y = f(x)$. Ou seja, todo elemento de B é imagem de algum elemento em A. Dizemos que B é a imagem de f e denotamos por $B = im(f)$.

Uma função também será dita sobrejetiva se $f(A) = B$. Para obter algumas propriedades importantes com relação a imagens de subconjuntos de A por f consulte Lima (2013, p. 17-18).

Exemplo 4.12 A função $f: \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 2x + 1$ é sobrejetiva. Com efeito, dado um $y \in \mathbb{R}$, existe $x \in \mathbb{R}$, $x = \frac{y-1}{2}$, tal que, $f(x) = f\left(\frac{y-1}{2}\right) = 2 \cdot \frac{y-1}{2} + 1 = (y - 1) + 1 = y$.

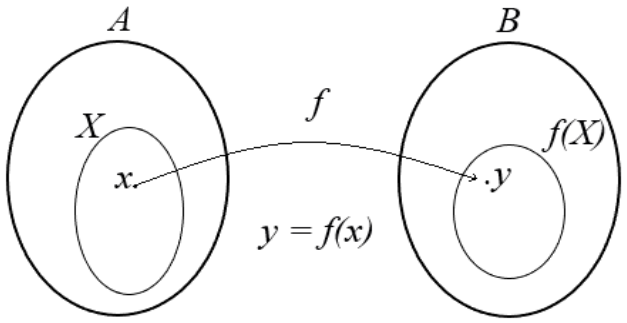
Definição 4.12 Uma função $f: A \to B$ é dita bijetiva se for injetiva e sobrejetiva simultaneamente.

Exemplo 4.13 A função $f: \mathbb{R} \to \mathbb{R}$ dada por $f(x) = 2x + 1$ é bijetiva. É também bijetiva a função $f: \mathbb{R}^+ \to \mathbb{R}^+$ dada por $f(x) = x^2$. A sobrejetividade dela é provada em Lima (2013).

Exemplo 4.14 A função $f: \mathbb{R} \to \mathbb{R}$ dada por $f(x) = |x|$, onde $|x|$ denota o valor absoluto de x, não é injetiva, pois, por exemplo, $f(-1) = |-1| = |1| = f(1)$. Portanto, f não é bijetiva.

Seja dada uma função $f: A \to B$ e um subconjunto $X \subset A$. Chama-se imagem de X por f o conjunto de todos os elementos $f(x)$, onde $x \in X$. Isto é, $f(X) = \{f(x) \in B; x \in X\}$.

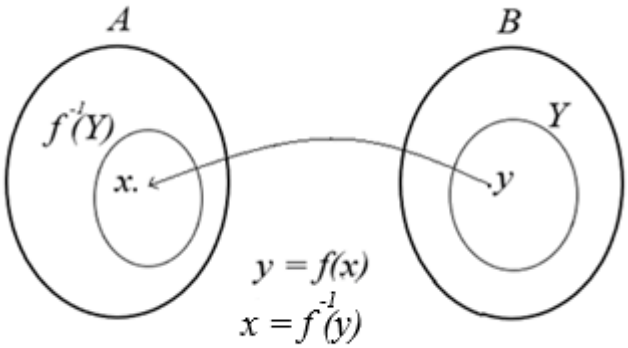
Figura 16 – Imagem de um Conjunto por meio de uma Função f



Fonte: Autoria própria

A imagem inversa de um subconjunto $Y \subset B$ será definida como sendo o conjunto de todos os $x \in A$ tais que $f(x) \in Y$. Esse conjunto é indicado na literatura por $f^{-1}(Y)$. Isto é, $f^{-1}(Y) = \{x \in A; f(x) \in Y\}$.

Figura 17 – Imagem inversa de um Conjunto por meio de uma Função f

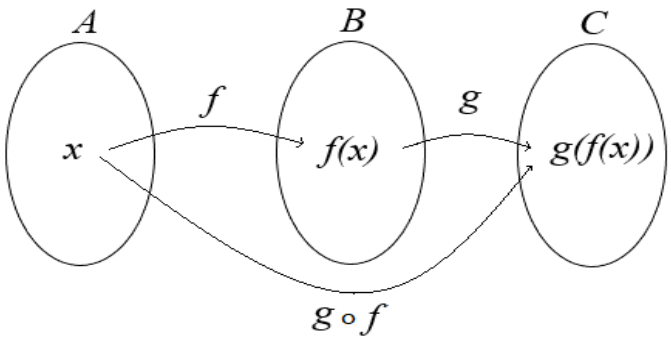


Fonte: Autoria própria

Para obter algumas propriedades importantes com relação a imagens inversas de subconjuntos $Y \subset B$ por f consulte Lima (2013, p. 19-20).

Outra operação importante entre funções é a operação de composição. Em Dante (2011), Capítulo 2, o leitor encontrará uma rica fonte de informações sobre funções em nível de ensino básico, onde a função composta é definida da seguinte forma: "dadas as funções $f: A \to B$ e $g: B \to C$, denominamos função composta de g e f a função $g \circ f: A \to C$, que é definida por $(g \circ f)(x) = g\big(f(x)\big),\ x \in A$" (DANTE, 2011, p. 50).

Figura 18 – Composição de Funções



Fonte: Autoria própria

Exemplo 4.15 Dadas as funções $f: \mathbb{R} \to \mathbb{R}$, tal que, $f(x) = x^2$ e $g: \mathbb{R}^+ \to \mathbb{R}$, tal que $g\ (x) = \sqrt{x}$, teremos $g \circ f: \mathbb{R} \to \mathbb{R}$ dada por $(g \circ f)(x) = g\big(f(x)\big) = \sqrt{x^2} = |x|$.

Finalizaremos estas considerações sobre funções apresentando o importante conceito de função inversa. Para isso, vamos entender o que é função inversa à direita e função inversa à esquerda para uma função $f: A \to B$.

Definição 4.13 Uma função $g: B \to A$ será dita uma *inversa à esquerd*a para f se $(g \circ f)(x) = g\big(f(x)\big) = x$ para todo $x \in A$. De modo análogo, $g: B \to A$ será dita uma *inversa à direita* para f se $(f \circ g)(x) = f\big(g(x)\big) = y$ para todo $y \in B$. Por fim, se $g: B \to A$ for uma inversa à direita e à esquerda para $f: A \to B$, diremos simplesmente que g é uma $inversa$ para f.

Exemplo 4.16 Dadas as funções $f: \mathbb{R}^+ \to \mathbb{R}^+$, tal que, $f(x) = x^2$ e $g: \mathbb{R}^+ \to \mathbb{R}^+$, definida por $g(x) = \sqrt{x}$, teremos: $(g \circ f)(x) = g\big(f(x)\big) = \sqrt{x^2} = |x| = x$. E, por sua vez, $(f \circ g)(x) = f\big(g(x)\big) = (\sqrt{x})^2 = x$. Logo, g é uma inversa para f.

Teorema 4.1 Uma função $f: A \to B$ admite inversa à esquerda se, e somente se, for injetiva, e inversa à direita se, e somente se, for sobrejetiva.

Teorema 4.2 Se a função f tem por inversa à direita a função g e por inversa à esquerda a função h, então $g = h$ é a função inversa de f, e f será dita *invertível.*

Os Teoremas 4.1 e 4.2 nos ensina que uma função f admite inversa se, e somente se, é bijetiva, e essa inversa, caso exista, é única. Para indicar a função inversa de $f: A \to B$ usamos a notação $f^{-1}: B \to A$. Para uma demonstração destes teoremas, consulte Lima (2013).

4.1.3 Criptossistemas

Ao desenvolvermos nosso breve estudo sobre criptografia nos capítulos anteriores, já nos deparamos com *Criptossistemas,* só que com outra denominação. O que chamamos de criptossistema em criptografia nada mais é do que um método geral de criptografia (descrito formalmente e bem caracterizado), ou algoritmo criptográfico como havíamos chamado. Também chamados de "esquema de codificação criptográfica" (BUCHMANN, 2002, p. 85), os criptossistemas são definidos da seguinte forma.

Definição 4.14 (*Criptossistemas*) Dá-se o nome de criptossistema a toda lista $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, onde $\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}$ e $\mathcal{D}$ são conjuntos não vazios, com as seguintes características:

a) O conjunto $\mathcal{P}$ tem por elementos todos os textos originais que desejamos codificar. Esses textos originais também são chamados de textos comuns. Segundo Buchmann (2002), o conjunto $\mathcal{P}$ denomina-se espaço de texto comum (ou *plaintext*);
b) Quando codificamos um texto comum $x \in \mathcal{P}$ obtemos outro texto, cifrado, y. O conjunto de todos os $y's$ obtidos através dos $x's$ em $\mathcal{P}$ é o conjunto $\mathcal{C}$. "Ele é chamado de espaço de texto cifrado. Seus elementos são chamados de textos cifrados (*Ciphertext*)" (BUCHMANN, 2002, p. 85);
c) O conjunto $\mathcal{K}$ é formado por todas as chaves possíveis do criptossistema;

d) Para cada chave $\alpha \in \mathcal{K}$ utilizada, isto é, para cada maneira específica de codificarmos um texto comum, podemos associar uma função $E_\alpha: \mathcal{P} \rightarrow \mathcal{C}$ que associa a cada texto comum $x \in \mathcal{P}$ um texto cifrado $y \in \mathcal{C}$, tal que $E_\alpha(x) = y$. A igualdade $E_\alpha(x) = y$ significa que quando codificarmos o texto x utilizando a chave α, obteremos o texto cifrado y. O conjunto $\mathcal{E}$ será o conjunto de todas essas funções E_α ($\mathcal{E} = \{E_\alpha; \alpha \in \mathcal{K}\}$). Os elementos de $\mathcal{E}$ serão chamados de funções de codificação criptográficas;

e) Para cada chave $\alpha \in \mathcal{K}$, existe uma chave $\beta \in \mathcal{K}$ associada e uma função $D_\beta: \mathcal{C} \rightarrow \mathcal{P}$ que faz corresponder a cada texto cifrado y o texto comum x a ele correspondente. Temos $D_\beta(y) = x$. O texto x é recuperado através de y e da chave β. $\mathcal{D}$ será o conjunto de todas essas funções D_β ($\mathcal{D} = \{D_\beta; \beta \in \mathcal{K}$). Os elementos de $\mathcal{D}$ serão chamados de funções de decodificação criptográfica;

f) A chave α é a chave de codificação criptográfica, e a chave β é a chave de decodificação criptográfica associada à α. Para cada $\alpha \in \mathcal{K}$ deve existir uma chave $\beta \in \mathcal{K}$, tal que $D_\beta\big(E_\alpha(x)\big) = x$. Ou seja, sempre que codificarmos um texto comum x utilizando α, devemos ser capazes de recuperar x decodificando $E_\alpha(x)$ por meio da chave β. Isto mostra que a função D_β é uma inversa à esquerda para a função E_α. Como a igualdade $E_\alpha\left(D_\beta(y)\right) = y$ é óbvia, segue que D_β é uma inversa à direita para a função E_α. Portanto, *D_β é a função inversa de E_α*.

Observação 4.1 Como nosso propósito neste trabalho não é desenvolver os aspectos teóricos da criptografia, a definição acima serve apenas para destacar os conceitos matemáticos envolvidos. O leitor deve perceber o quanto de clareza, rigor e objetividade a definição ganhou com o uso de ideias básicas de conjuntos e funções. Sem problema algum a linguagem utilizada para caracterizar os criptossistemas é compreendida por qualquer pessoa que tenha o domínio básico de linguagem de conjuntos e funções. Essa simplicidade da criptografia proporcionada pela matemática básica pode ser apreciada por meio de outros temas, tais como matrizes e probabilidades. Teremos a oportunidade de apreciar isso, mais adiante, neste capítulo.

Exemplo 4.17 Como exemplo, vamos explorar mais uma vez a cifra de César (Capítulo 2, Secção 2.1.3). Ela é um criptossistema. Para provarmos isso, devemos nos certificar que essa cifra possui todas as características apresentadas na Definição 4.14. De fato:

a) A cifra de César codifica letra por letra. Logo, o conjunto $\mathcal{P}$ (espaço de texto comum) é o conjunto {A, B, C, ..., Z} de todas as letras do nosso alfabeto usual;
b) A cifra de César é de substituição, que associa a cada letra de $\mathcal{P}$ outra letra também de $\mathcal{P}$. Portanto, o conjunto $\mathcal{C}$(espaço de texto cifrado) também é o conjunto {A, B, C, ..., Z}.
c) Sabemos que há 26 possíveis chaves para a cifra de César. Uma vez que cada chave corresponde ao número de letras transladadas da esquerda para a direita (e esse número varia de 1 á 26), podemos dizer que as chaves possíveis para a cifra de César são os números 1, 2, 3, 4, ..., 25, 26. Por exemplo, se usarmos a chave $\alpha = 7$, então o alfabeto será transladado 7 casas à direita. Assim sendo, $\mathcal{K} = \{1,2,3,4,5, \dots ,26\}$.
d) Para verificarmos a característica (d) da Definição 4.14 iremos associar a cada letra do alfabeto usual os números de 1 à 26 segundo a Tabela 8.

Tabela 8 - Tabela de Pré-codificação

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

Fonte: Autoria própria

Com a ajuda da Tabela 8 e do que aprendemos sobre congruências no Capítulo 3, podemos descrever as funções de codificação e decodificação criptográfica para a cifra de César. Iniciemos com a função de codificação. Dada uma chave $\alpha \in \mathcal{K} = \{1,2,3,4,5, \dots ,26\}$, a função de codificação criptográfica vai associar a cada letra de $\mathcal{P}$ uma outra letra de $\mathcal{P}$, obtida transladando o alfabeto α casas à frente. Logo, se

$x \in \mathcal{P}$ é um texto comum (uma letra, que neste caso passará a ser um número de 1 à 26 pela Tabela 8), o texto cifrado $y \in \mathcal{C}$ (mesma observação do caso de x) será dado por:

$$y \equiv x + \alpha \ (mod. 26)$$

Ou seja, a função $E_\alpha: \mathcal{P} \to \mathcal{C}$ é tal que $E_\alpha(x) = y \equiv x + \alpha \ (mod. 26)$. Portanto,

$$\mathcal{E} = \{E_\alpha; \alpha \in \mathcal{K} \text{ e } E_\alpha(x) \equiv x + \alpha \ (mod. 26)\}.$$

Observação 4.2 Lembre-se que x, y *e* α são inteiros positivos pertencentes ao conjunto {1, 2, 3, ..., 26}. Assim, a congruência $y \equiv x + \alpha \ (mod. 26)$ nos diz que y será igual ao resto da divisão de $x + \alpha$ por 26, que é uma maneira mais formal de apresentarmos as translações da cifra de César. Para entendermos melhor o porquê da função de codificação ser escolhida desta forma, suponhamos que a chave $\alpha = 12$. Isto quer dizer que o alfabeto será transladado 12 casas à frente. Qual letra representará a codificação da letra W? Pela Tabela 8, temos que W = 23. Logo, 23 + 12 = 35. Assim, a letra W será substituída pela letra de número 35. Entretanto, as letras estão representadas até o número 26. Mas como 35 = 26 + 9, isto significa que contamos até a letra de número 26 (letra Z), depois voltamos ao inicio do alfabeto e contamos mais nove casas (letras). Ou seja, a letra correspondente ao W será a letra de número 9, letra I. Note que $9 \equiv 23 + 12 \ (mod. 26)$ por isso, consideramos a congruência módulo 26 (contamos de 26 em 26).

e) Como para decodificar a cifra de César basta apenas reverter a translação, segue que se $\beta \in \mathcal{K}$, então a função de decodificação associada à β será dada por:

$$x \equiv y - \beta \ (mod. 26)$$

Ou seja, a função D_β: $\mathcal{C} \to \mathcal{P}$ é tal que $D_\beta(y) = x \equiv y - \beta \ (mod. 26)$. Portanto, temos que $\mathcal{D} = \{D_\beta; \ \beta \in \mathcal{K} \text{ e } D_\beta(y) \equiv y - \beta \ (mod. 26)\}$. Como na cifra de César as chaves de codificação e decodificação são iguais, segue que $\alpha = \beta$ e a função de decodificação passar a ser apenas $D_\beta(y) = x \equiv y - \alpha (mod. 26)$. Assim, por exemplo, no caso da Observação 4.2, com $\alpha = 12$, vemos que $\beta = 12$ é a chave de decodificação e $D_{12}(9) \equiv 9 - 12 = -3 \equiv 23 (mod. 26)$. Logo, decodificando a letra de número 9 (letra I), obtemos a letra de número 23 (letra W), isto é, recuperamos a letra W que tinha sido codificada.

f) Por fim, é óbvio que para toda chave $\alpha \in \mathcal{K}$, existe uma chave $\beta \in \mathcal{K}$, com $\alpha = \beta$, tal que $D_\beta\big(E_\alpha(x)\big) = x$, qualquer que seja o texto comum $x \in \mathcal{P}$.

O exposto nos itens anteriores prova que a cifra de César é um criptossistema. Outro exemplo muito importante de criptossistema é o RSA. Para mais detalhes, veja Buchmann (2002). A seguir, trataremos das noções de alfabetos e palavras em criptografia.

4.1.4 Alfabetos e Palavras

Já temos uma boa noção do que sejam alfabetos e palavras em criptografia. Porém, rigorosamente falando, esses conceitos assumem um significado mais geral que difere do usual utilizado por nós no dia a dia. Como já sabemos, para que possamos escrever uma mensagem ou um texto comum precisamos utilizar um alfabeto. No nosso caso, o alfabeto usual utilizado é {A, B, C, ..., Z}. No entanto, esse não é o único alfabeto possível, e as palavras e os textos assumirão características que dependem, logicamente, do alfabeto utilizado. Por exemplo, já vimos dois exemplos clássicos de alfabetos: o alfabeto Morse e o alfabeto Braille. A definição a seguir baseia-se na dada por Buchmann (2002).

Definição 4.15 Chama-se *Alfabeto* todo conjunto $\mathcal{A}$ finito e não vazio. Se $\mathcal{A}$ tem n elementos, dizemos que o *Comprimento* de $\mathcal{A}$ é igual a n. Os elementos de $\mathcal{A}$ são chamados de *Letras* ou *Símbolos*.

Exemplo 4.18

a) $\mathcal{A} = \{A, B, C, D, \dots, Z\} =$ Alfabeto usual. Comprimento de $\mathcal{A}$ é igual a 26;
b) $\mathcal{A} = \{0, 1\} =$ Alfabeto binário. Comprimento de $\mathcal{A}$ é igual a 2;
c) $\mathcal{A} = \{símbolos\ ASCII\}$ (ver Tabela 17). Comprimento de $\mathcal{A}$ é igual a 128.

Observação 4.3 Se considerarmos, como fizemos antes, a associação apresentada na Tabela 8, podemos interpretar o alfabeto $\{A, B, C, D, \dots, Z\}$ como sendo o conjunto {1, 2, 3, ..., 26}. Isto é muito usado em criptografia, pois permite "calcular com letras". Em geral, podemos fazer essa associação com qualquer alfabeto $\mathcal{A}$. Ou seja, se $\mathcal{A}$ tem comprimento m, então podemos associar aos símbolos de $\mathcal{A}$ os números 1, 2, 3,..., m, ou de maneira análoga aos números 0, 1, 2, ..., $m - 1$, o que dá no mesmo (BUCHMANN, 2002).

As definições a seguir, baseadas em Buchmann (2002), nos fornecem a noção formal de *Palavra* em criptografia e alguns conceitos relacionados.

Definição 4.16 Seja $\mathcal{A}$ um alfabeto qualquer. Chamamos de *palavra* (em $\mathcal{A}$) qualquer sequência finita formada por símbolos de $\mathcal{A}$. O espaço entre palavras também está incluso e passará a ser chamado de sequência vazia.

Exemplo 4.19 Se $\mathcal{A} = \{0, 1\}$, então $m = 1001101011$ é uma palavra em $\mathcal{A}$.

Definição 4.17 Cada símbolo que compõe uma palavra num alfabeto $\mathcal{A}$ será chamado de componente da palavra. Se uma palavra tem n componentes, diremos que o comprimento dessa palavra é n.

Exemplo 4.20 Seja $\mathcal{A} = \{A, B, C, D, \dots, Z\}$. A palavra UFERSA tem comprimento 6 em $\mathcal{A}$. Analogamente, a palavra $m = 1001101011$ do alfabeto $\mathcal{A} = \{0, 1\}$, dada no Exemplo 4.19, tem comprimento igual a 10.

Definição 4.18 Seja $\mathcal{A}$ um alfabeto qualquer. O conjunto de todas as palavras que podem ser formadas com os símbolos de $\mathcal{A}$, incluindo a sequência vazia, será denotado por $\mathcal{A}^*$. Da mesma forma, o conjunto de todas as palavras de comprimento fixo n em $\mathcal{A}$ será denotado por $\mathcal{A}^{(n)}$.

Exemplo 4.21 Seja $\mathcal{A} = \{A, B, C, D, \dots, Z\}$. Apenas com os símbolos de $\mathcal{A}$, quantas palavras podemos formar? Quantas dessas palavras tem comprimento 4? Ora, podemos ter palavras com 1 símbolo, 2 símbolos, 3 símbolos, e assim por diante, até as palavras de 26 símbolos. Existem 26 palavras com 1 símbolo, 26 x 26 palavras com 2 símbolos, 26 x 26 x 26 palavras com 3 símbolos, ..., 26 x 26 x ... x 26 (26 fatores) palavras com 26 símbolos em $\mathcal{A}$. Logo, a quantidade de palavras que podemos formar com os símbolos de $\mathcal{A}$ é:

$$26 + 26^2 + 26^3 + \cdots + 26^{26}.$$

Se incluirmos a sequência vazia, temos uma quantidade de

$$1 + 26 + 26^2 + 26^3 + \cdots + 26^{26} = \frac{26^{27} - 1}{26 - 1} = \frac{26^{27} - 1}{25}$$

palavras formadas com os símbolos de $\mathcal{A} = \{A, B, C, D, \dots, Z\}$. Assim, $\mathcal{A}^*$ tem $\frac{26^{27}-1}{25}$ elementos. A quantidade de palavras com comprimento 4 é 26^4. Logo, $\mathcal{A}^{(4)}$ tem 26^4 elementos.

4.1.5 Permutações

A análise combinatória, tão explorada no Ensino Médio, ganha importância em criptografia por meio da noção de *Permutação*. Esta noção é a base para o desenvolvimento das *Cifras em Blocos*, que definiremos mais adiante. Ao leitor interessado em relacionar análise combinatória com criptografia, sugerimos uma consulta a Malagutti (2015).

O problema das permutações é um dos problemas centrais de que se ocupa a análise combinatória. Ele é basicamente o seguinte: De quantas formas podemos dispor em fila n objetos distintos? Ou seja, considerando $X = \{x_1, x_2, \dots, x_n\}$ um conjunto com n elementos distintos, de quantos modos podemos dispor em fila todos os elementos de X? A cada uma dessas disposições damos o nome de permutação dos elementos $x_1, x_2, \dots, x_n$.

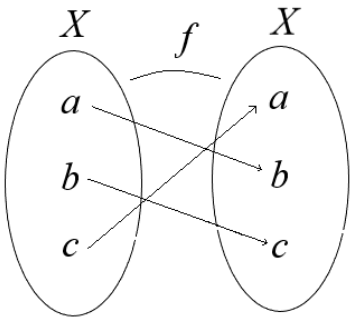
Exemplo 4.22 Seja $X = \{a, b, c\}$. As permutações dos elementos de X são: $(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)$.

Podemos formalizar a ideia de permutação da seguinte forma:

Definição 4.19 Seja X um conjunto não vazio. Chamamos de permutação dos elementos de X a qualquer função bijetiva $f: X \to X$.

Exemplo 4.23 Seja $X = \{a, b, c\}$. Uma permutação dos elementos de X pode ser obtida considerando a função bijetiva $f: X \to X$ definida por $f(a) = b, f(b) = c$ e $f(c) = a$. No Exemplo 4.22 esta permutação se refere a (b, c, a). Assim, há 6 bijeções $f: X \to X$. A Figura 19 a seguir ilustra a associação entre os elementos de X de modo a ter uma bijeção $f: X \to X$.

Figura 19 – Um exemplo de Permutação



Fonte: Autoria própria

É também comum indicarmos essa permutação assim: $\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$.

As permutações que aparecem com mais frequência em criptografia são as dos elementos do conjunto $I_n = \{1, 2, 3, 4, \dots, n\}$. Denotaremos por S_n o conjunto de todas as permutações possíveis dos elementos de I_n. Sabemos da análise combinatória que o número de permutações de n elementos distintos é igual a $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$. Portanto, o número de permutações dos elementos de I_n é igual a $n!$. Ou seja, S_n tem $n!$ elementos.

Exemplo 4.24 S_3 é o conjunto de todas as permutações de $I_3 = \{1, 2, 3\}$ e possui $3! = 6$ elementos, que são: (1, 2, 3), (1, 3, 2), (3, 1, 2), (2, 1, 3), (2, 3, 1), (3, 2, 1).

A seguir, iremos estudar as cifras em blocos e analisar como o conceito básico de permutação está inserido na definição dessas cifras.

4.1.6 Cifras em Blocos

As cifras em blocos, como o nome sugere, são aquelas que codificam em blocos, isto é, codificam palavras de comprimento fixo n ($n \in \mathbb{N}$). No Capítulo 1, estudamos cifras em que a codificação era realizada letra por letra (cifras de substituição) individualmente. Nas cifras de blocos podemos codificar qualquer sequência finita de letras de mesmo comprimento e do mesmo alfabeto considerado. Passemos à definição formal:

Definição 4.20 Um método criptográfico (criptossistema) é chamado de *cifra de blocos* (ou *cifras em blocos*) se seu espaço de texto comum e o seu espaço de texto cifrado correspondem ao conjunto $\mathcal{A}^{(n)}$ das palavras formadas por n símbolos do alfabeto $\mathcal{A}$ (BUCHMANN, 2002). Se uma cifra em blocos codifica palavras de comprimento n, dizemos que essa cifra tem comprimento de bloco igual a n.

Exemplo 4.25 A cifra de César é uma cifra em blocos. Seu comprimento de bloco é igual a 1 porque ela codifica palavras de comprimento 1 em palavras de comprimento também igual a 1. Outro exemplo, mais geral, de cifras em blocos são as cifras de substituição.

O teorema a seguir, cuja demonstração pode ser encontrada em Buchmann (2002, p. 94) explicita a importância das permutações para as cifras em blocos.

Teorema 4.3 Nas cifras em blocos, as funções de codificação criptográfica são permutações.

Um dos casos mais simples de cifras em blocos consiste naquele onde a função de codificação criptográfica associa a cada palavra $(l_1, l_2, \dots, l_n)$[34] $\in \mathcal{A}^{(n)}$ a palavra $(l_{\pi(1),} l_{\pi(2),} \dots, l_{\pi(n)}) \in \mathcal{A}^{(n)}$, onde $(\pi(1), \pi(2), \dots, \pi(n))$ é uma permutação dos elementos do conjunto $I_n = \{1, 2, 3, 4, \dots, n\}$, isto é, $(\pi(1), \pi(2), \dots, \pi(n)) \in S_n$. Ou seja, o que esta cifra faz é apenas permutar os componentes da palavra $(l_1, l_2, \dots, l_n)$. Daí, temos que essas cifras também são chamadas de cifras de permutação.

Exemplo 4.26 Vamos considerar o alfabeto $\mathcal{A} = \{A, B, C, D, \dots, Z\}$. Uma cifra em blocos, de comprimento n, pode ser definida da seguinte forma: A cada palavra $(l_1, l_2, \dots, l_n) \in \mathcal{A}^{(n)}$ associamos a palavra $(l_{\pi(1),} l_{\pi(2),} \dots, l_{\pi(n)}) \in \mathcal{A}^{(n)}$, onde $(\pi(1), \pi(2), \dots, \pi(n))$ é uma permutação dos elementos 1, 2, ..., n. Neste caso, o espaço das chaves é o conjunto de todas as permutações de I_n, isto é, o conjunto S_n. Ou seja, as chaves para essa cifra são as permutações $\pi: \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. Portanto, dada uma chave $\pi \in S_n$, temos que a função de codificação criptográfica será

$$E_\pi: \mathcal{A}^{(n)} \to \mathcal{A}^{(n)};\ (l_1, l_2, \dots, l_n) \mapsto \left(l_{\pi(1)}, l_{\pi(2)}, \dots, l_{\pi(n)}\right).$$

Por outro lado, a função de decodificação criptográfica será:

$$D_\pi: \mathcal{A}^{(n)} \to \mathcal{A}^{(n)}; (x_1, x_2, \dots, x_n) \mapsto \left(x_{\pi^{-1}(1)}, x_{\pi^{-1}(2)}, \dots, x_{\pi^{-1}(n)}\right),$$

onde $\pi^{-1}: \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ é a função inversa da função π.

Exemplo 4.27. No Exemplo 4.26, façamos $n = 4$. Ou seja, vamos definir uma cifra em blocos de comprimento 4 sobre $\mathcal{A} = \{A, B, C, D, \dots, Z\}$. Então, tomemos uma chave $\pi \in S_4$. Seja $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ (π é *a permutação* $(2, 1, 4, 3)$). Vamos codificar a palavra (A, M, O, R) por meio da cifra descrita no Exemplo 4.26. Ora, neste caso, $l_1 = A$, $l_2 = M$, $l_3 = O$ e $l_4 = R$. Por sua vez, $l_{\pi(1)} = l_2 = M$, $l_{\pi(2)} = l_1 = A$, $l_{\pi(3)} = l_4 = R$ e $l_{\pi(4)} = l_3 = O$. Ou seja, a função de codificação criptográfica E_π vai associar à palavra (A, M, O, R) a palavra (M, A, R, O). Portanto, $E_\pi(A, M, O, R) = (M, A, R, O)$ e a palavra AMOR será transformada em MARO. Por outro lado, para decodificar a palavra (M, A, R, O) basta fazer: $x_1 = M$, $x_2 = A$, $x_3 = R$ e $x_4 = O$. Logo, $x_{\pi^{-1}(1)} = x_2 = A$, $x_{\pi^{-1}(2)} = x_1 = M$,

[34] Notação que usaremos para indicar uma palavra de comprimento fixo num alfabeto $\mathcal{A}$.

$x_{\pi^{-1}(3)} = x_4 = O$ e $x_{\pi^{-1}(4)} = x_3 = R$. Assim, a função de decodificação criptográfica D_π vai associar à palavra (M, A, R, O) a palavra (A, M, O, R). Portanto, $D_\pi(M, A, R, O) = (A, M, O, R)$ e a decodificação está encerrada.

Na seção a seguir estaremos interessados em ampliar nossa investigação acerca das aplicações de funções ao campo da criptografia. Para isto, revisaremos um tipo muito importante de função, conhecido como Função Afim, e buscaremos desenvolver uma relação simples entre essas funções e um método bem elementar de criptografia. Na Seção 4.3, onde revisaremos outro tipo especial de função, as Funções Quadráticas, esta aplicação também se dará.

4.2 Funções Afins e Criptografia

Uma Função Afim é toda função $f: \mathbb{R} \to \mathbb{R}$, tal que, existem números reais a e b com $f(x) = ax + b$. Quando $a = 0$, temos a função constante $f(x) = b$ que é um caso particular de Função Afim. Outros exemplos de Funções Afins são: $f(x) = ax$, (no caso em que temos $b = 0$ e $a \neq 0$) $f(x) = 2x + 1$, $f(x) = x + b$ ($Função\ Translação$), etc. Outros conceitos relacionados à teoria das Funções Afins, como gráfico, taxa de variação e teorema de caracterização, por exemplo, não serão tratados aqui. Para o que segue, o exposto na Seção 4.1 sobre funções é suficiente. Para o leitor interessado em revisar as noções básicas sobre Função Afim, e outras funções elementares vistas no ensino básico, indicamos as obras: Giovanni Júnior *et al*. (2018), Bianchini (2018), Balestri (2016), Iezzi *et al*. (2002), Lima *et al*. (2006a) e Dante (2006). Logicamente, no caso do professor, a primeira referência é o livro didático. Para melhor desenvolver essa relação entre criptografia e matemática, o professor deve preparar sua abordagem de acordo com a sequência do livro utilizado pela turma e no tempo certo para não ocorrer de precisar de ferramentas que só serão vistas muito posteriormente.

Portanto, nesta seção, nosso objetivo é apresentar um exemplo bem didático (e intuitivo) de uma cifra utilizando as Funções Afins. O valor didático desse exemplo reside no fato de que podemos trabalhar várias noções básicas sobre essas funções, tais como: definição (exibir exemplos de Funções Afins), imagem de um elemento do domínio, cálculo da Função Inversa, imagem inversa de um elemento, etc. O professor pode ampliar as aplicações desse exemplo, buscando relacionar outros conceitos. Por exemplo, em França (2014), Capítulo 3,

pode-se encontrar atividades que exploram vários conceitos relacionados às Funções Afins (e outras funções) por meio de um exemplo de método de criptografia baseado na função em questão. Por esse motivo, sugerimos ao leitor a consulta a esse trabalho. Esta seção e a Seção 4.3 são fortemente inspiradas no Capítulo 3 de França (2014).

4.2.1 Um método criptográfico intuitivo baseado em Funções Afins

Inicialmente, iremos utilizar mais uma vez a Tabela 8 de pré-codificação. O método criptográfico que apresentamos possui como espaço de texto comum o alfabeto {1, 2, 3, 4, ..., 26}. Ele é uma cifra de blocos com comprimento 1, isto é, codifica letra por letra. Seu espaço de texto cifrado é um subconjunto (finito) de $\mathbb{N}$. Ou seja, cada letra será codificada em um número. Assim, a mensagem codificada passa a ser representada por uma sequência de números separados por um traço (parecido com a separação de blocos no RSA). A seguir, apresentamos um guia de desenvolvimento e aplicação do método.

Roteiro 1 – Processo de codificação do método

Etapa 1: Nesta etapa iremos escolher, como exemplo, uma mensagem curta para ser codificada por um método criptográfico simples baseado em funções afins. Assim, suponhamos que queremos codificar a mensagem CRIPTOGRAFIA NO PROFMAT. A vantagem desse método é que sua simplicidade torna possível utilizar exemplos de codificação com mensagens longas sem se preocupar com cálculos extensos. Logo, é uma ótima alternativa para trabalhar em sala de aula com variados tipos de exemplos.

Etapa 2: Aqui inicia-se o processo de pré-codificação. Usando a Tabela 8, substituímos cada letra da mensagem CRIPTOGRAFIA NO PROFMAT pelo número que lhe é correspondente, separando-os por um traço (-). Logo, a mensagem passará a ser:

3-18-9-16-20-15-7-18-1-6-9-1-14-15-16-18-15-6-13-1-20.

Etapa 3: Aqui iremos utilizar o conhecimento sobre funções afins para desenvolver um processo de codificação criptográfica, isto é, uma função de codificação criptográfica. A função de codificação que iremos utilizar será uma Função Afim. Para obtê-la, começamos escolhendo um par ordenado (a, b) (com a e b inteiros para evitar números fracionários, raízes, etc). Depois, consideraremos a função de codificação criptográfica como sendo $f(x) = ax + b$, onde a variável x, de acordo com a Tabela 8, será um número natural

pertencente ao conjunto $\{1, 2, 3, \ldots, 26\}$. Sendo assim, tomemos, por exemplo, o par (2, 1) como chave de codificação, isto é, nossa função de codificação será $f(x) = 2x + 1$.

Etapa 4 Da Etapa 2 temos que a mensagem CRIPTOGRAFIA NO PROFMAT passa a ser representada pela sequência de números (blocos)

3-18-9-16-20-15-7-18-1-6-9-1-14-15-16-18-15-6-13-1-20.

Da Etapa 3 temos que cada um desses blocos será codificado por meio da função $f(x) = 2x + 1$, onde iremos calcular a imagem de cada número que compõe a mensagem. Cada uma dessas imagens será a codificação do número (bloco) correspondente. Devemos respeitar a sequência dos números, e os resultados devem ser separados por traço na mesma ordem. Esta nova sequência é a codificação da mensagem original.

Agora utilizaremos nosso conhecimento sobre cálculo do valor de uma Função Afim num ponto x para codificar cada bloco da mensagem original. Calculando a imagem de cada bloco da mensagem 3-18-9-16-20-15-7-18-1-6-9-1-14-15-16-18-15-6-13-1-20, obtemos:

Tabela 9 – Codificando a Mensagem

Bloco (x)	**Função de codificação** $(f(x) = 2x + 1)$	**Bloco codificado** $(y = f(x))$
3	$f(3) = 2 \cdot 3 + 1 = 7$	7
18	$f(18) = 2 \cdot 18 + 1 = 37$	37
9	$f(9) = 2 \cdot 9 + 1 = 19$	19
16	$f(16) = 2 \cdot 16 + 1 = 33$	33
20	$f(20) = 2 \cdot 20 + 1 = 41$	41
15	$f(15) = 2 \cdot 15 + 1 = 31$	31
7	$f(7) = 2 \cdot 7 + 1 = 15$	15
14	$f(14) = 2 \cdot 14 + 1 = 29$	29
6	$f(6) = 2 \cdot 6 + 1 = 13$	13

13	$f(13) = 2 \cdot 13 + 1 = 27$	27
1	$f(1) = 2 \cdot 1 + 1 = 3$	3

Fonte: Autoria própria

Daí, a mensagem codificada passará a ser:

7-37-19-33-41-31-15-37-3-13-19-3-29-31-33-37-31-13-27-3-41.

Substituímos cada número pela sua imagem por meio da função $f(x) = 2x + 1$.

Portanto, a mensagem CRIPTOGRAFIA NO PROFMAT será substituída por:

7-37-19-33-41-31-15-37-3-13-19-3-29-31-33-37-31-13-27-3-41.

Veja que, nestas condições, a chave utilizada para codificar a mensagem foi o par ordenado (2, 1). Mas, por que fixamos esse par como ordenado? Porque no caso em que $a \neq b$, temos que $(a, b) \neq (b, a)$. Logo, temos duas chaves distintas!

Roteiro 2 – Processo de decodificação do método

Codificada a mensagem, nosso proceder agora será desenvolver a função de decodificação criptográfica para o nosso método. Ora, se o bloco x foi substituído por sua imagem $f(x)$, o que devemos fazer para recuperar x? Como sabemos do estudo sobre funções, x é recuperado quando calculamos a imagem inversa dele. Ou seja, se $y = f(x)$, então $x = f^{-1}(y)$ (é a imagem de y pela função inversa de f). Portanto, para decodificarmos a mensagem, precisamos saber a função inversa da função de codificação (claro, se ela existir). No caso da função afim, a sua inversa sempre vai existir, pois as funções afins são bijetivas.

Etapa 1: Bom, temos que a função de codificação criptográfica é $f(x) = 2x + 1$. Então, devemos determinar a função inversa da função $f(x) = 2x + 1$. Isolando x nessa igualdade, temos $x = \frac{f(x)-1}{2} = \frac{y-1}{2}$. Segue então que $f^{-1}(y) = \frac{y-1}{2}$. Portanto, a função inversa de f é $f^{-1}(x) = \frac{x-1}{2}$.

Etapa 2: Como já temos a função de decodificação criptográfica, basta calcular a imagem de cada número na mensagem codificada para obter a mensagem original. Ou seja, calcularemos a imagem de cada número na sequência

7-37-19-33-41-31-15-37-3-13-19-3-29-31-33-37-31-13-27-3-41

por meio da função $f^{-1}(x) = \frac{x-1}{2}$. Isso é mostrado na tabela a seguir.

Tabela 10 – Decodificando a Mensagem

Bloco (y)	**Função de decodificação** $(f^{-1}(y) = \frac{y-1}{2})$	**Bloco codificado** $(x = f^{-1}(y))$
7	$f^{-1}(7) = \frac{7-1}{2} = \frac{6}{2} = 3$	3
37	$f^{-1}(37) = \frac{37-1}{2} = \frac{36}{2} = 18$	18
19	$f^{-1}(19) = \frac{19-1}{2} = \frac{18}{2} = 9$	9
33	$f^{-1}(33) = \frac{33-1}{2} = \frac{32}{2} = 16$	16
41	$f^{-1}(41) = \frac{41-1}{2} = \frac{40}{2} = 20$	20
31	$f^{-1}(31) = \frac{31-1}{2} = \frac{30}{2} = 15$	15
15	$f^{-1}(15) = \frac{15-1}{2} = \frac{14}{2} = 7$	7
29	$f^{-1}(29) = \frac{29-1}{2} = \frac{28}{2} = 14$	14
13	$f^{-1}(13) = \frac{13-1}{2} = \frac{12}{2} = 6$	6
27	$f^{-1}(27) = \frac{27-1}{2} = \frac{26}{2} = 13$	13

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

Fonte: Autoria própria

Assim, tendo decodificado cada número, fica fácil recuperar a mensagem. Basta substituir os números na mensagem 7-37-19-33-41-31-15-37-3-13-19-3-29-31-33-37-31-13-27-3-41 codificada por seus correspondentes na tabela anterior. A mensagem torna-se então:

3-18-9-16-20-15-7-18-1-6-9-1-14-15-16-18-15-6-13-1-20.

Por meio da tabela de pré-codificação (Tabela 8), podemos observar as letras correspondentes a esses números e obter a mensagem original.

CRIPTOGRAFIA NO PROFMAT.

Agora um detalhe técnico: como a função de decodificação consiste na inversa da função $f(x) = 2x + 1$, temos que a chave de decodificação é $(\frac{1}{2}, -\frac{1}{2})$, pois $f^{-1}(x) = \frac{x-1}{2} = \frac{1}{2}x - \frac{1}{2}$. De modo geral, se codificarmos uma mensagem com chave (a, b), com $a \neq 0$, temos que a chave de decodificação será $(\frac{1}{a}, -\frac{b}{a})$, pois se $a \neq 0$, a inversa da função $f(x) = ax + b$ é $f^{-1}(x) = \frac{x-b}{a} = \frac{1}{a}x + \left(-\frac{b}{a}\right)$.

Os Exemplos 4.28 e 4.29 a seguir trazem mais algumas alternativas para explorar a relação entre criptografia e funções afins por meio do método descrito anteriormente. Juntos, os roteiros desenvolvidos nesta seção e os Exemplos 4.28 e 4.29 constituem um excelente guia para tratar a relação entre funções afins e criptografia em sala de aula, trabalhando os conceitos matemáticos envolvidos por meio da resolução de problemas e codificação criptográfica.

Exemplo 4.28 Codifique com base na Tabela 8 e na chave (3, 10), a mensagem: O SEGREDO DO COFRE É SUA DATA DE NASCIMENTO.

Solução: Com base na tabela de pré-codificação, a mensagem dada torna-se a seguinte sequência de blocos:

15-19-5-7-18-5-4-15-4-15-3-15-6-18-5-5-19-21-1-4-1-20-1-4-5-14-1-19-3-9-13-5-14-20-15.

Como a chave de codificação é função de codificação (3, 10), segue que a função de codificação criptográfica é a função $f(x) = 3x + 10$. Assim, calculando a imagem de todos os números que aparecem na sequência anterior, correspondente à mensagem original, teremos:

Tabela 11 – Codificação da Mensagem do Exemplo 4.28

x	1	3	4	5	6	7	9	13	14	15	18	19	20	21
$f(x)$	13	19	22	25	28	31	37	49	52	55	64	67	70	73

Fonte: Autoria própria

Logo, a mensagem codificada será dada por:

55-67-25-31-64-25-22-55-22-55-19-55-28-64-25-25-67-73-13-22-13-70-13-22-25-52-13-67-19-37-49-25-52-70-55.

Exemplo 4.29 Vamos supor que um estudante A está utilizando esse método de criptografia com funções afins para mandar mensagens secretas para outro estudante B na sala de aula. Um terceiro estudante, C, está interessado em saber o conteúdo das mensagens trocadas por A e B. No entanto, C não possui a chave de decodificação envolvida no processo, pois ele é um intruso nessa situação. Obstinado a quebrar o código utilizado por A e B, C descobriu, de alguma forma, que por meio da função de codificação utilizada por A, o 1 passa a ser o 52, e o 5 passa a ser 188. Pergunta-se: com essa nova informação, C tem condições de quebrar o código utilizado pelos estudantes A e B? Suponha que C sabe que o método utilizado por A e B é este baseado em funções afins, e que a tabela de pré-codificação é a mesma que a apresentada nesta seção.

Solução: Sim! Veja por que: como C sabe que A e B estão codificando usando uma função do tipo $f(x) = ax + b$, então ele sabe que basta conhecer os valores de a e b para obter as funções de codificação e decodificação criptográficas. Ora, com a informação que C possui, ele pode concluir que $f(1) = 52$ e $f(5) = 188$. Logo, substituindo essas informações na expressão $f(x) = ax + b$, obtêm-se: $a + b = 52$ e $5a + b = 188$. Portanto, para saber os valores de a e b, C só precisa resolver o sistema a seguir:

$$\begin{cases} a + b = 52 \\ 5a + b = 188 \end{cases}$$

Subtraindo a primeira equação da segunda, temos $4a = 188 - 52 = 136$. O que implica que $a = \frac{136}{4} = 34 \Rightarrow b = 52 - a = 52 - 34 = 18$. Daí, C conclui que $a = 34$ e $b = 18$. Logo, a função utilizada para criptografar as mensagens é $f(x) = 34x + 18$. Com esta função em mãos, o estudante C pode facilmente decifrar as mensagens trocas por A e B. Claro, supondo que A e B não modifiquem algum elemento na utilização desse método de criptografia.

A seguir, apresentaremos outro exemplo didático de um método intuitivo utilizando funções. Desta vez, trataremos da Função Quadrática.

4.3 Funções Quadráticas e Criptografia

Uma Função Quadrática (ou Função Polinomial do 2º grau) é toda função $f: \mathbb{R} \to \mathbb{R}$, tal que, existem números reais a, b e c, sendo $a \neq 0$, com $f(x) = ax^2 + bx + c$. Quando $b = c = 0$, temos a função quadrática $f(x) = ax^2$ que é o caso mais simples de tais funções. Alguns exemplos de funções quadráticas são: $f(x) = ax^2 + bx$ $(no\ caso\ em\ que\ c = 0)$, $f(x) = ax^2 + c$, $(quando\ b = 0)$, etc. Lembrando sempre que o coeficiente a deve ser diferente de zero para que tenhamos certeza que a função $f(x) = ax^2 + bx + c$ é quadrática.

Se tratando da Teoria das Funções Quadráticas, deixaremos de abordar grande parte dos conceitos habitualmente vistos no ensino básico. A razão para isso, como já explicitado, é que tais conceitos não são necessários para o desenvolvimento e entendimento do conteúdo exposto. Trataremos de mencionar aquilo que realmente importa e que assume um papel central na aplicação de criptografia apresentada. Assim sendo, temas como: gráfico, forma canônica, teorema de caracterização, valores máximos e mínimos, etc., não serão desenvolvidos como de costume. Quando necessário, faremos menção a algum desses conceitos diretamente no texto em que o mesmo for citado, ou então em nota de rodapé. No caso do leitor interessado em revisar o assunto, as mesmas referências dadas na Seção 4.2 também servem para um estudo introdutório sobre Funções Quadráticas.

4.3.1 Um método criptográfico intuitivo baseado em Funções Quadráticas

Semelhante ao que fizemos na Seção 4.2, nosso propósito nesta seção é descrever um método bem elementar de criptografia com base na Função Quadrática[35]. Para isto, nossa tabela de pré-codificação continua sendo a mesma usada no caso da Função Afim. Para o método criptográfico que apresentamos, valem as mesmas informações dadas para o método da seção anterior, isto é, ele possui espaço de texto comum {1, 2, 3, 4, ..., 26}, ele é uma cifra de blocos com comprimento 1 e seu espaço de texto cifrado é um subconjunto finito de $\mathbb{N}$. O roteiro apresentado a seguir é semelhante ao desenvolvido na Seção 4.3.1 para funções afins. Por isso, seremos mais sucintos no desenvolvimento do roteiro para evitar repetições de ideias.

Roteiro 1 – Processo de codificação do método

Etapa 1: Suponhamos que queremos codificar a mensagem A VIDA É UM SOPRO. Usando a Tabela 8, substituímos cada letra pelo número que lhe é correspondente, separando-os por um traço (-), como fizemos na Seção 4.2. Logo, a mensagem passará a ser:

1-22-9-4-1-5-21-13-19-15-16-18-15.

Etapa 2: Agora, precisamos codificar cada número (bloco) que forma a mensagem. Entra em cena a questão da escolha da função de codificação criptográfica. No caso presente, esta função será a Função Quadrática $f(x) = ax^2 + bx + c$ $(a \neq 0)$ com domínio restringido ao conjunto {1, 2,, ..., 26}. Então, começamos escolhendo os coeficientes a, b e c. Em termos de chave de codificação, isto significa escolher uma tripla ordenada (a, b, c) de números reais (que no nosso caso serão escolhidos de modo que os valores da função sejam naturais, para simplificar e evitar exageros). Escolhemos então a chave (2, 1, 1). Ou seja, vamos utilizar a função $f(x) = 2x^2 + x + 1$ como função de codificação criptográfica.

Etapa 3: Escolhida a função de codificação criptográfica $f(x) = 2x^2 + x + 1$, basta calcular a imagem de cada número da sequência que forma a mensagem original, que pela Etapa 1 é

1-22-9-4-1-5-21-13-19-15-16-18-15.

[35] Rigorosamente falando, e isto se aplica também para o caso já tratado utilizando Função Afim, não usamos realmente uma Função Quadrática, de acordo com a definição dada. Isso porque o domínio utilizado por nós não é o conjunto dos números reais. O que fazemos é restringir o domínio da função ao conjunto {1, 2, 3, .., 26} e usar como lei de formação desta função a expressão $f(x) = ax^2 + bx + c$. Mas isto não representa nenhum incomodo para a descrição e aplicação do método estudado.

A Tabela 12 a seguir resume os cálculos realizados.

Tabela 12 – Codificando a Mensagem

Bloco (x)	**Função de codificação** $(f(x) = 2x^2 + x + 1)$	**Bloco codificado** $(y = f(x))$
1	$f(1) = 2 \cdot 1^2 + 1 + 1 = 4$	4
22	$f(22) = 2 \cdot 22^2 + 22 + 1 = 991$	991
9	$f(9) = 2 \cdot 9^2 + 9 + 1 = 172$	172
4	$f(4) = 2 \cdot 4^2 + 4 + 1 = 37$	37
5	$f(5) = 2 \cdot 5^2 + 5 + 1 = 56$	56
21	$f(21) = 2 \cdot 21^2 + 21 + 1 = 904$	904
13	$f(13) = 2 \cdot 13^2 + 13 + 1 = 352$	352
19	$f(19) = 2 \cdot 19^2 + 19 + 1 = 742$	742
16	$f(16) = 2 \cdot 16^2 + 16 + 1 = 529$	529
18	$f(18) = 2 \cdot 18^2 + 18 + 1 = 667$	667
15	$f(15) = 2 \cdot 15^2 + 15 + 1 = 466$	466

Fonte: Autoria própria

A mensagem codificada passará a ser a sequência de blocos:

4-991-172-37-4-56-904-352-742-466-529-667-466.

Roteiro 2 – Processo de decodificação do método

Para recuperarmos a mensagem original necessitamos da função de decodificação criptográfica. Ora, já sabemos que essa função é a inversa da função de codificação. Então, temos que calcular a inversa da função $f(x) = 2x^2 + x + 1$. Aqui esbarramos num ponto importante. Como vimos na Seção 4.1, a fim de que uma função tenha inversa é necessário, e suficiente que ela seja bijetiva. É de nosso conhecimento que a função quadrática não é bijetiva em toda a reta, isto é, em $\mathbb{R}$, por não ser injetiva[36]. Porém, é fácil vencer esta dificuldade. Basta considerar a função definida em um dos intervalos $(-\infty, x_v]$ ou $[x_v, +\infty)$, pois neste caso a função será bijetiva. x_v indica a abcissa do vértice da parábola, gráfico da função quadrática em questão. A imagem (que será igual ao contradomínio) da função será $[y_v, +\infty)$ quando $a > 0$, e $(-\infty, y_v]$ quando $a < 0$.[37] Onde y_v indica a ordenada do vértice da parábola, gráfico da função quadrática em questão. Voltando ao caso da função de codificação, o gráfico da mesma é uma parábola com vértice $(-\frac{1}{4}; \frac{7}{8})$. Como só atribuímos valores naturais para x, segue que o domínio de f está contido em $[-\frac{1}{4}, +\infty)$, segue então que existe a inversa de f. Portanto, existe a função de decodificação criptográfica. Como é fácil ver, o domínio da inversa de f será um subconjunto de $[\frac{7}{8}, +\infty)$. Calculemos então a função inversa de f. Essa será nossa Etapa 1 do processo de decodificação.

Etapa 1: Temos que $f(x) = y = 2x^2 + x + 1$ é a função de codificação criptográfica. Queremos calcular x em função de y. A igualdade

$$y = 2x^2 + x + 1$$

torna-se a equação do segundo grau $2x^2 + x + 1 - y = 0$ na incógnita x (caso seja necessário, é importante revisar as equações do 2º grau e o método de resolução utilizado a seguir). Calculando as raízes dessa equação em função de y, teremos:

$$x = \frac{-1 \pm \sqrt{1^2 - 4.2.(1-y)}}{4} = \frac{-1 \pm \sqrt{1 - 8(1-y)}}{4}$$

$$\Longrightarrow x = \frac{-1 + \sqrt{1 - 8(1-y)}}{4} \text{ ou } x = \frac{-1 - \sqrt{1 - 8(1-y)}}{4}.$$

[36]Como o gráfico da função quadrática é uma parábola, dois elementos do domínio, simétricos em relação a abcissa do vértice dessa parábola, terão mesma imagem. Logo, a função é injetiva em $\mathbb{R}$.

[37] Os símbolos x_v *e* y_v representam, respectivamente, a abcissa e a ordenada do vértice da parábola, gráfico da função quadrática f.

Como o domínio de f é $[-\frac{1}{4}, +\infty)$, segue que $x = \frac{-1+\sqrt{1-8(1-y)}}{4}$.

Portanto, temos que

$$x = f^{-1}(y) = \frac{-1+\sqrt{1-8(1-y)}}{4}.$$

A função inversa de f, com domínio $\left[\frac{7}{8}, +\infty\right)$, é:

$$f^{-1}(x) = \frac{-1+\sqrt{1-8(1-x)}}{4}.$$

Etapa 2: Nesta etapa realizamos o processo de decodificação dos blocos que constituem a mensagem original codificada. Sendo $f^{-1}(x) = \frac{-1+\sqrt{1-8(1-x)}}{4}$ a função de decodificação, basta aplicá-la aos blocos que forma a mensagem codificada para obter a mensagem original. Não faremos as contas aqui, mas o leitor pode se certificar de que realmente recuperamos todos os blocos codificados calculando a imagem de todos os números na mensagem codificada por meio de f^{-1}. Por exemplo, o primeiro bloco da mensagem codificada é 4. Logo, para decodificar esse bloco, basta substituí-lo na função f^{-1}, obtendo

$$f^{-1}(4) = \frac{-1+\sqrt{1-8(1-4)}}{4} = \frac{-1+\sqrt{1-8(-3)}}{4} = \frac{-1+\sqrt{1+24}}{4} = \frac{-1+5}{4} = 1.$$

Ou seja, o bloco original correspondente ao bloco 4 é o 1. Repetindo esses cálculos para todos os blocos, recuperamos a mensagem. A tabela a seguir resume o processo de decodificação:

Tabela 13 – Decodificando a Mensagem

y	4	991	172	37	56	904	352	742	529	667	466
$f^{-1}(y)$	1	22	9	4	5	21	13	19	16	18	15

Fonte: Autoria própria

A mensagem decodificada passa a ser a sequência 1-22-9-4-1-5-21-13-19-15-16-18-15 que corresponde à mensagem original A VIDA É UM SOPRO pela Tabela 8, e o processo está encerrado.

O exemplo a seguir trata de um caso simples do método desenvolvido nesta seção e pode ser bastante utilizado em sala de aula para exercitar as noções de quadrados perfeitos e raízes quadradas.

Exemplo 4.30 (A função $f(x) = x^2$**)** Neste exemplo, nossa função de codificação criptográfica é $f: \mathbb{R}^+ \to \mathbb{R}^+$dada por $f(x) = x^2$. Note que esta função é quadrática, com mesma lei de formação, porém com domínio e contradomínio restringidos ao conjunto dos números reais não negativos. Assim, existe a função de decodificação, pois a função é bijetiva. Neste exemplo, podemos trabalhar não só a ideia de Função Quadrática (no ensino médio), mas também os conceitos de quadrados de números naturais, radiciação e operações inversas (no ensino fundamental). Pretendemos criptografar a mensagem A MATEMÁTICA É A RAINHA DAS CIÊNCIAS usando como método elementar as Funções Quadráticas. Em particular, utilizaremos a função $f: \mathbb{R}^+ \to \mathbb{R}^+$ dada por $f(x) = x^2$. Usando a Tabela 8, a mensagem original será convertida em:

1-13-1-20-5-13-1-20-9-3-1-5-1-18-1-9-14-8-1-4-1-19-3-9-5-14-3-9-1-19.

Agora, para codificar a mensagem precisamos calcular o quadrado dos números que a forma, isto é, calcular a imagem de cada bloco da mensagem pela função $f(x) = x^2$. A tabela a seguir resume esses simples cálculos:

Tabela 14 – Codificação da Mensagem do Exemplo 4.30

x	1	13	20	5	9	3	18	14	8	4	19
x^2	1	169	400	25	81	9	324	196	64	16	371

Fonte: Autoria própria

A mensagem criptografada será:

1-169-1-400-25-169-1-400-81-9-1-25-1-324-1-81-196-64-1-16-1-371-9-81-25-196-9-81-1-371.

Para recuperarmos a mensagem, necessitamos da função inversa de f. Como sabemos, a operação inversa da potenciação é a radiciação. Logo, a função inversa de $f(x) = x^2$ é $f(x) = \sqrt{x}$ (veja que como $\sqrt{x}$ não está definido para $x < 0$, necessitamos restringir o contradomínio de f à $\mathbb{R}^+$). Precisamos calcular a raiz quadrada de todos os números que formam a mensagem codificada (esta é uma ótima oportunidade para treinar o cálculo de raízes quadradas). Teremos então a seguinte tabela:

Tabela 15 – Decodificação da Mensagem do Exemplo 4.30

y	1	169	400	25	81	9	324	196	64	16	371
$\sqrt{y}$	1	13	20	5	9	3	18	14	8	4	19

Fonte: Autoria própria

Substituindo os blocos na mensagem codificada por seus correspondentes, decodificados, obtemos:

1-13-1-20-5-13-1-20-9-3-1-5-1-18-1-9-14-8-1-4-1-19-3-9-5-14-3-9-1-19.

Que representa a mensagem A MATEMÁTICA É A RAINHA DAS CIÊNCIAS. O processo está encerrado!

Observação 4.3 Na prática em sala de aula, o professor pode explorar mais exemplos como esses com o intuito de revisar e exercitar tópicos já estudados. No caso anterior, estávamos tratando de funções, mas o exemplo nos levou a revisar outras noções igualmente importantes. Assim, com base no que fizemos no exemplo anterior, podemos trabalhar com potências de expoentes mais altos, assim como trabalhar com raízes cúbicas, quartas, quintas, etc., sem contar, claro, que podemos ampliar esses exercícios de criptografia para o caso de outras funções, como as polinomiais de grau n, funções racionais, exponenciais, logarítmicas, etc. Como é fácil ver através dos exemplos analisados anteriormente, não é necessário falar em função para trabalharmos com exemplos semelhantes em sala de aula no ensino fundamental. Digamos que estamos no fundamental e os alunos não conhecem ainda as funções. O professor pode, e deve quando necessário, adaptar as atividades ao nível e bagagem de conhecimento da turma. Assim, sem mencionar funções, o professor pode, por exemplo, trabalhar fórmulas ou expressões algébricas e desenvolver atividades/exercícios, semelhantes àqueles desenvolvidos com funções, envolvendo criptografia. Desse modo, temos a oportunidade de inserir o assunto criptografia nas séries iniciais do ensino fundamental. É só uma questão de adaptação!

Na seção a seguir, investigaremos um pouco a relação entre matrizes e os métodos criptográficos.

4.4 Matrizes e Criptografia

Apesar das aplicações de Matrizes à Criptografia serem mais bem exploradas (e entendidas) no campo da Álgebra Linear, é possível tratarmos de aspectos elementares dessas aplicações somente com os conceitos básicos sobre Matrizes, visto num curso básico de matemática. Portanto, nesta seção faremos uma breve revisão sobre o conceito e as propriedades das matrizes, finalizando com uma aplicação muito interessante em criptografia, a cifra de Hill.

4.4.1 Algumas noções sobre Matrizes

Definição 4.21. Dados os números naturais m e n, uma Matriz real $A = [a_{ij}]$ de ordem m por n é um quadro (tabela) formado por mxn números reais dispostos em m linhas e n colunas. O elemento genérico a_{ij} da matriz A se encontra na intersecção da i-ésima linha com a j-ésima coluna de A.

Uma Matriz $A = [a_{ij}]$ de ordem m por n é usualmente representada por:

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}.$$

Para indicar a Matriz $A = [a_{ij}]$ de ordem m por n usaremos a notação mais simples $A = [a_{ij}]_{mxn}$, bem comum nos livros de ensino médio. A seguir apresentaremos algumas matrizes especiais por meio de exemplos.

Exemplo 4.31 (*Matriz Linha* e *Matriz Coluna*) Uma Matriz que só possui uma linha, isto é, uma matriz $A = [a_{ij}]_{1xn}$, é chamada de Matriz Linha. Uma denominação semelhante é dada às matrizes com apenas uma coluna.

Exemplo 4.32 (*Matriz Nula*) Chama-se Matriz Nula toda Matriz $A = [a_{ij}]_{mxn}$ tal que $a_{ij} = 0$ para todo $1 \leq i \leq m$ e todo $1 \leq j \leq n$. Ou seja, Matriz Nula é aquela que só possui elementos nulos. Iremos indicar a Matriz Nula de ordem m por n pelo símbolo $\mathcal{O}_{mxn}$,

$$\mathcal{O} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}.$$

Exemplo 4.33 (*Matriz Quadrada*) Uma classe muito importante de matrizes são as chamadas Matrizes Quadradas. Uma Matriz $A = [a_{ij}]_{mxn}$ chama-se quadrada quando possui o número de linhas igual ao número de colunas, isto é, $m = n$. Neste caso, dizemos apenas Matriz quadrada A de ordem m. A Matriz a seguir é quadrada de ordem 3:

$$A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}.$$

Definição 4.22 A diagonal principal de uma Matriz quadrada A de ordem m é o conjunto dos elementos a_{ij} com $i = j$. Ou seja, é o conjunto $\{a_{11}, a_{22}, \dots, a_{mm}\}$. Da mesma forma, chama-se diagonal secundária o conjunto dos elementos a_{ij} com $i + j = m + 1$, a saber, o conjunto $\{a_{1m}, a_{2(m-1)}, \dots, a_{m1}\}$.

Exemplo 4.34 A diagonal principal e a diagonal secundária da Matriz A a seguir são, respectivamente, os conjuntos {1, 7, 9} e {3, 5, 7}.

$$A = \begin{bmatrix} 1 & 4 & 5 \\ 2 & 7 & 8 \\ 3 & 6 & 9 \end{bmatrix}.$$

Exemplo 4.35 (*Matriz Diagonal*) Quando em uma Matriz quadrada $A = [a_{ij}]$ de ordem m todos os elementos que não estão na diagonal principal são nulos, isto é, $a_{ij} = 0$ para $i \neq j$, a mesma é chamada de Matriz Diagonal.

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 9 \end{bmatrix} \qquad \mathcal{O}_{2x2} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Em particular, a Matriz Nula quadrada de ordem m é uma Matriz Diagonal.

Exemplo 4.36 (*Matriz Identidade*) Matriz Identidade de ordem m, simbolizada por $\mathbb{I}_m$, é toda Matriz diagonal em que $a_{ij} = 1$ para $i = j$. Ou seja, Matriz Identidade é uma Matriz Diagonal onde na diagonal principal só consta elementos iguais a 1.

$$\mathbb{I}_m = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Definição 4.23 (*Igualdade de Matrizes*) Dadas as matrizes $A = [a_{ij}]_{mxn}$ e $B = [b_{ij}]_{mxn}$, diremos que $A = B$ quando $a_{ij} = b_{ij}$ para todo $1 \leq i \leq m$ e todo $1 \leq j \leq n$. Ou seja, para que duas matrizes A e B sejam iguais é necessário, e suficiente, que sejam de mesma ordem e que os elementos correspondentes (aqueles que ocupam o mesmo lugar nas matrizes) sejam iguais.

Exemplo 4.37 Para que a matriz $M = \begin{bmatrix} 2 & 5 \\ 7 & 11 \end{bmatrix}$ seja igual à matriz $N = \begin{bmatrix} 2 & x \\ y+1 & 11 \end{bmatrix}$ devemos ter $x = 5$ e $y = 6$.

Denotando por $\mathcal{M}(mxn)$ o conjunto das matrizes $A = [a_{ij}]_{mxn}$, é sabido que podemos definir operações nesse conjunto muito semelhantes às operações com números reais, por exemplo. Iremos revisar as operações de Adição, Subtração e Multiplicação de matrizes, multiplicação de uma matriz por um número real e inversa de uma matriz.

Definição 4.24 (*Adição de Matrizes*) Dadas as matrizes $A = [a_{ij}]_{mxn}$ e $B = [b_{ij}]_{mxn}$, chama-se Matriz Soma de A e B, a Matriz $M + N = [a_{ij} + b_{ij}]$ de ordem $m\ por\ n$, formada somando os elementos correspondentes em A e B.

Exemplo 4.38 Considere as matrizes $A = \begin{bmatrix} -5 & 8 \\ 3 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix}$. Temos:

$$A + B = \begin{bmatrix} -5 & 8 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 4 & 5 \end{bmatrix} = \begin{bmatrix} -4 & 10 \\ 7 & 9 \end{bmatrix}.$$

Definição 4.25 (*Diferença de Matrizes*) A Matriz Simétrica (ou oposta) de $A = [a_{ij}]_{mxn}$ é a Matriz $-A = [-a_{ij}]_{mxn}$ tal que $A + (-A) = (-A) + A = \mathcal{O}_{mxn}$. Chama-se Matriz diferença das matrizes $A = [a_{ij}]_{mxn}$ e $B = [b_{ij}]_{mxn}$ a Matriz $M + (-N) = [a_{ij} + (-b_{ij})]$, obtida somando A com a Matriz simétrica de B.

Exemplo 4.39 Considere as matrizes $A = \begin{bmatrix} -5 & 8 \\ 3 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} -7 & 2 \\ 4 & 3 \end{bmatrix}$. Temos:

$$A - B = A + (-B) = \begin{bmatrix} -5 & 8 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 7 & -2 \\ -4 & -3 \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ -1 & 1 \end{bmatrix}.$$

Definição 4.26 (*Multiplicação de um número real por uma Matriz*) Dados um número real α e uma Matriz $A = [a_{ij}]_{mxn}$, chama-se Matriz produto de α por A a Matriz $\alpha \cdot A = [\alpha . a_{ij}]_{mxn}$formada multiplicando todos os elementos de A pelo número real α.

Exemplo 4.40 Se $\alpha = 4$ e $A = \begin{bmatrix} 3 & 2 \\ 1 & 0 \end{bmatrix}$, então $\alpha \cdot A = 4 \cdot \begin{bmatrix} 3 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 4 \cdot 3 & 4 \cdot 2 \\ 4 \cdot 1 & 4 \cdot 0 \end{bmatrix} = \begin{bmatrix} 12 & 8 \\ 4 & 0 \end{bmatrix}$.

Definição 4.27 (*Multiplicação de Matrizes***)** Dadas as matrizes $A = [a_{ij}]_{mxn}$ e $B = [b_{jk}]_{nxp}$, chama-se Matriz Produto de A por B, a Matriz $A \cdot B = [c_{ik}]$ de ordem m por p, onde $c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + a_{i3}b_{3k} + \cdots + a_{in}b_{nk}$, com $1 \leq i \leq m$ e $1 \leq k \leq p$. Ou seja, para dar origem ao elemento c_{ik} da Matriz $A \cdot B$ multiplicamos a *i*-ésima linha de A pela *k*-ésima coluna de B.

Observação 4.4 A multiplicação de $A = [a_{ij}]_{mxn}$ por $B = [b_{jk}]_{qxp}$só está definida no caso em que o número de colunas de A for igual ao número de linhas de B $(n = q)$. Daí, a matriz $A \cdot B$ terá m linhas e p colunas.

Exemplo 4.41 Seja $A = \begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix}$ e $B = \begin{bmatrix} 2 & 7 & 0 \\ 3 & -4 & 11 \end{bmatrix}$. Tem-se:

$$A \cdot B = \begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} 2 & 7 & 0 \\ 3 & -4 & 11 \end{bmatrix} = \begin{bmatrix} 2 \cdot 2 + 0 \cdot 3 & 2 \cdot 7 + 0 \cdot (-4) & 2 \cdot 0 + 0 \cdot 11 \\ 1 \cdot 2 + 3 \cdot 3 & 1 \cdot 7 + 3 \cdot (-4) & 1 \cdot 0 + 3 \cdot 11 \end{bmatrix} = \begin{bmatrix} 4 & 14 & 0 \\ 11 & -5 & 33 \end{bmatrix}.$$

Exemplo 4.42 Dada a Matriz $A = [a_{ij}]_{mxn}$e as matrizes identidades $\mathbb{I}_n$ e $\mathbb{I}_m$, temos $A \cdot \mathbb{I}_n = \mathbb{I}_m \cdot A = A$. Com efeito, seja c_{ik} um elemento genérico de $A \cdot \mathbb{I}_n$. Tem-se:

$$c_{ik} = a_{i1} \cdot 0 + a_{i2} \cdot 0 + \cdots + a_{i,(k-1)} \cdot 0 + a_{ik}I_{kk} + a_{i,(k+1)} \cdot 0 + \cdots + a_{in} \cdot 0.$$

Onde I_{ik} é um elemento genérico de $\mathbb{I}_n$. Logo, $c_{ik} = a_{ik}I_{kk} = a_{ik} \cdot 1 = a_{ik}$. Donde concluímos que $A.\cdot \mathbb{I}_n = A$. De modo análogo prova-se que $\mathbb{I}_m \cdot A = A$.

Definição 4.28 (Matriz Invertível) Seja $A = [a_{ij}]$ uma Matriz quadrada de ordem m. Se existir uma Matriz B tal que $A \cdot B = B \cdot A = \mathbb{I}_m$, então A é dita Invertível.

Observação 4.5 A Matriz B na definição anterior, quando existe, é única. Com efeito, se existisse outra Matriz C tal que $A \cdot C = C \cdot A = \mathbb{I}_m$, então

$$C = C \cdot \mathbb{I}_m = C \cdot (A \cdot B) = (C.A).B = \mathbb{I}_m.B = B.$$

Da mesma forma, $C = \mathbb{I}_m \cdot C = (B \cdot A) \cdot C = B \cdot (A \cdot C) = B \cdot \mathbb{I}_m = B$. Portanto, $C = B$, o que mostra que B é única.

Exemplo 4.43 Seja $A = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix}$. A Matriz $B = \begin{bmatrix} 7 & -3 \\ -2 & 1 \end{bmatrix}$ é tal que $A \cdot B = B \cdot A = \mathbb{I}_2$. Logo, A é invertível.

Definição 4.29 Seja dada uma Matriz $A = [a_{ij}]$ invertível de ordem m. A matriz B tal que $A \cdot B = B \cdot A = \mathbb{I}_m$ chama-se Inversa da Matriz A e será denotada por $B = A^{-1}$. Portanto, $A \cdot A^{-1} = A^{-1} \cdot A = \mathbb{I}_m$.

Do exposto anteriormente temos que se a inversa da matriz A existe, então ela é única. Assim, A é invertível se admite inversa. É claro que A^{-1} também deve ser uma matriz quadrada de ordem m, caso contrário não faria sentido a igualdade $A \cdot A^{-1} = A^{-1} \cdot A$.

Exemplo 4.44 A inversa da matriz $A = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix}$ é $A^{-1} = \begin{bmatrix} 1 & -\frac{3}{2} \\ 0 & 1/2 \end{bmatrix}$. Com efeito, seja $A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Da igualdade $A \cdot A^{-1} = \mathbb{I}_2$, temos:

$$\begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix} . \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Longrightarrow \begin{bmatrix} a+3c & b+3d \\ 2c & 2d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Pela condição de igualdade de matrizes, teremos as igualdades: $2c = 0$ *e* $2d = 1$. Logo, $c = 0$ e $d = \frac{1}{2}$. Temos também $a + 3c = 1 \Rightarrow a = 1$, e $b + 3d = 0 \Rightarrow b + \frac{3}{2} = 0 \Rightarrow b = -\frac{3}{2}$.

Conclusão: $a = 1, b = -\frac{3}{2}, c = 0$ e $d = \frac{1}{2}$. Assim, $A^{-1} = \begin{bmatrix} 1 & -\frac{3}{2} \\ 0 & \frac{1}{2} \end{bmatrix}$.

4.4.2 A Cifra de Hill

Outro método clássico de criptografia é a chamada Cifra de Hill. Esta cifra foi inventada em 1929 por Lester S. Hill, e se baseia em Álgebra Linear e Aritmética Modular. Veja, por exemplo, Howard e Horres (2001), Capítulo 11, Seção 11.16. Nossa descrição aqui frisa o aspecto teórico básico desta cifra no que tange as operações básicas com matrizes. Nesse sentido, as obras Tavares *et al*. (2017), Loureiro (2014), Brandão (2017) e Jesus (2013)

são ótimas referências. Uma abordagem mais ampla pode ser encontrada nos livros de criptografia, por exemplo, Buchmann (2002).

A cifra de Hill é uma cifra em blocos. Logo, antes de codificarmos a mensagem, a mesma é dividida em blocos. Consideremos então uma mensagem M a ser codificada. No caso do alfabeto utilizado ser o usual, substituímos todas as letras da mensagem por seus valores numéricos de acordo com a Tabela 8. Em seguida, escolhemos a chave de codificação, que será uma matriz quadrada A, invertível, de ordem n e com todos os elementos inteiros. A mensagem M é então dividida em blocos de tamanho n. Cada bloco desses será representado por uma matriz coluna

$$\begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_n \end{bmatrix}.$$

Onde $(b_1, b_2, b_3, \dots, b_n)$ é a sequência de letras que formam um bloco da mensagem. Para codificarmos o bloco $(b_1, b_2, b_3, \dots, b_n)$ multiplicamos a matriz A pela matriz anterior formada pelo bloco em questão, com a restrição de que os inteiros maiores que 25 nesse produto devem ser substituídos pelo seu resto na divisão por 26. A matriz produto obtida será do tipo nx1. A mensagem codificada será representada pela sequência de blocos codificados, seguindo a ordem dos blocos da mensagem original, isto é, não podemos trocar blocos de lugar. O exemplo a seguir ilustra este método. O mesmo será desenvolvido passo a passo como forma de guia para auxiliar o professor na aplicação em sala de aula.

Antes da aplicação de exemplos que envolvam qualquer método elementar de criptografia em sala de aula, é preciso verificar se os conceitos matemáticos envolvidos foram bem desenvolvidos e entendidos pelos alunos, pois assim os mesmos terão melhores condições de apreciar a matemática envolvida e exercitar os conceitos estudados. Desta forma, para uma boa aplicação da Cifra de Hill, o aluno deve possui pelo menos o conhecimento básico sobre matrizes, tipos especiais de matrizes, operações entre matrizes e matriz inversa (Cobrimos todo esse conteúdo na Seção 4.4.1). Assim, fica como primeira etapa para o professor, o desenvolvimento deste conteúdo como pré-requisito para a aplicação de atividades envolvendo a cifra em questão. Feito isso, podemos seguir o roteiro abaixo para trabalhar os processos de codificação e decodificação da Cifra de Hill.

Exemplo 4.45 Por meio da Cifra de Hill, iremos codificar, e posteriormente decodificar, a palavra MATEMÁTICA.

Roteiro 1 - Processo de codificação da Cifra de Hill

Etapa 1: Por simplicidade, vamos codificar a palavra MATEMÁTICA. É claro que a escolha é livre, mas palavras pequenas facilitam o entendimento da cifra e simplificam os cálculos realizados. Em termos didáticos isso é importante, pois caso contrário a utilização desta cifra em sala de aula pode ficar desinteressante e os cálculos enfadonhos.

Etapa 2: Nesta etapa começamos a pré codificar a palavra escolhida na Etapa 1. Por meio da Tabela 8, a palavra MATEMÁTICA passa a ser representada pela sequência de números 13-1-20-5-13-1-20-9-3-1.

Etapa 3: Nesta etapa devemos escolher a chave de codificação. Como visto anteriormente no texto, esta chave é uma matriz quadrada de ordem n só com elementos inteiros. Mais uma vez, por simplicidade, iremos escolher uma matriz quadrada A de ordem 2, como segue.

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

Etapa 4: Como a chave de codificação é uma matriz quadrada de ordem 2, então devemos dividir a sequência 13-1-20-5-13-1-20-9-3-1, obtida na Etapa 2, em blocos de comprimento 2:

(13-1)-(20-5)-(13-1)-(20-9)-(3-1).

Caso a mensagem tivesse um número impar de letras, e quiséssemos dividi-la em blocos de comprimento 2, poderíamos adicionar uma letra qualquer (ou símbolo) ao final da mesma.

Etapa 5: Os blocos obtidos na Etapa 4 passarão a ser representados, respectivamente, pelas seguintes matrizes-coluna:

$$\begin{bmatrix} 13 \\ 1 \end{bmatrix}, \begin{bmatrix} 20 \\ 5 \end{bmatrix}, \begin{bmatrix} 13 \\ 1 \end{bmatrix}, \begin{bmatrix} 20 \\ 9 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \end{bmatrix}.$$

Etapa 6: As etapas anteriores transformaram a palavra MATEMÁTICA em uma sequência de blocos representados por matrizes de ordem 2 x 1. Como sabemos, para realizar a codificação da mensagem original devemos codificar cada um desses blocos. A codificação de cada bloco será dada multiplicando a matriz-chave de codificação pela matriz que representa o bloco a ser codificado. Por isso, quando escolhemos a matriz-chave como sendo

quadrada de ordem 2 dividimos a sequência 13-1-20-5-13-1-20-9-3 em blocos de comprimento 2, pois assim a multiplicação da matriz-chave pela matriz-bloco pode ser realizada, veja Observação 4.4.

A codificação de cada um dos blocos $\begin{bmatrix}13\\1\end{bmatrix}, \begin{bmatrix}20\\5\end{bmatrix}, \begin{bmatrix}13\\1\end{bmatrix}, \begin{bmatrix}20\\9\end{bmatrix}, \begin{bmatrix}3\\1\end{bmatrix}$ será dada da seguinte forma:

Codificação do bloco $\begin{bmatrix}\mathbf{13}\\\mathbf{1}\end{bmatrix}$
Multiplicamos a matriz $\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}$ pela matriz $\begin{bmatrix}13\\1\end{bmatrix}$. Teremos: $$\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}\cdot\begin{bmatrix}13\\1\end{bmatrix}=\begin{bmatrix}1\cdot 13+0\cdot 1\\(-1)\cdot 13+2\cdot 1\end{bmatrix}=\begin{bmatrix}13+0\\-13+2\end{bmatrix}=\begin{bmatrix}13\\-11\end{bmatrix}$$

Codificação do bloco $\begin{bmatrix}\mathbf{20}\\\mathbf{5}\end{bmatrix}$
Multiplicamos a matriz $\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}$ pela matriz $\begin{bmatrix}20\\5\end{bmatrix}$. Teremos: $$\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}\cdot\begin{bmatrix}20\\5\end{bmatrix}=\begin{bmatrix}1\cdot 20+0\cdot 5\\(-1)\cdot 20+2\cdot 5\end{bmatrix}=\begin{bmatrix}20+0\\-20+10\end{bmatrix}=\begin{bmatrix}20\\-10\end{bmatrix}$$

Codificação do bloco $\begin{bmatrix}\mathbf{20}\\\mathbf{9}\end{bmatrix}$
Multiplicamos a matriz $\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}$ pela matriz $\begin{bmatrix}20\\9\end{bmatrix}$. Teremos: $$\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}\cdot\begin{bmatrix}20\\9\end{bmatrix}=\begin{bmatrix}1\cdot 20+0\cdot 9\\(-1)\cdot 20+2\cdot 9\end{bmatrix}=\begin{bmatrix}20+0\\-20+18\end{bmatrix}=\begin{bmatrix}20\\-2\end{bmatrix}$$

Codificação do bloco $\begin{bmatrix}\mathbf{3}\\\mathbf{1}\end{bmatrix}$
Multiplicamos a matriz $\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}$ pela matriz $\begin{bmatrix}3\\1\end{bmatrix}$. Teremos: $$\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}\cdot\begin{bmatrix}3\\1\end{bmatrix}=\begin{bmatrix}1\cdot 3+0\cdot 1\\(-1)\cdot 3+2\cdot 1\end{bmatrix}=\begin{bmatrix}3+0\\-3+2\end{bmatrix}=\begin{bmatrix}3\\-1\end{bmatrix}$$

Etapa 7: Das codificações da Etapa 6, temos que a sequência de blocos, que representa a mensagem original,

$$\begin{bmatrix}13\\1\end{bmatrix},\begin{bmatrix}20\\5\end{bmatrix},\begin{bmatrix}13\\1\end{bmatrix},\begin{bmatrix}20\\9\end{bmatrix},\begin{bmatrix}3\\1\end{bmatrix},$$

passa a ser codificada na sequência $\begin{bmatrix}13\\-11\end{bmatrix}$, $\begin{bmatrix}20\\-10\end{bmatrix}$,$\begin{bmatrix}13\\-11\end{bmatrix}$, $\begin{bmatrix}20\\-2\end{bmatrix}$, $\begin{bmatrix}3\\-1\end{bmatrix}$. Ou seja, a palavra MATEMÁTICA, codificada, será indicada pela sequência de blocos a seguir:

13-(-11)-20-(-10)-13-(-11)-20-(-2)-3-(-1).

Com o término da Etapa 7, o processo de codificação está encerrado. Note que não usamos a regra de substituir um número maior que 25 por seu resto na divisão por 26 no produto das matrizes. Isso se deu unicamente porque não obtivemos números maiores que 25. Mas como essa regra vale no geral para a cifra de Hill, é muito importante que a destaquemos. Logicamente, este é apenas um exemplo, e o leitor está livre para desenvolver os seus próprios com base no método geral e, se necessário, usar a regra. Vale a mesma observação para o processo de decodificação que realizaremos a seguir.

Roteiro 2 - Processo de decodificação da Cifra de Hill

Observação inicial: O processo de decodificação pode ser facilmente realizado, levando-se em consideração a seguinte observação: Para todas as matrizes A e B, sendo A invertível de ordem n, e B de ordem n por p, vale que:

$$A \cdot B = C \Leftrightarrow A^{-1} \cdot (A \cdot B) = A^{-1} \cdot C \Leftrightarrow B = A^{-1} \cdot C$$

Assim sendo, para recuperarmos os blocos da mensagem original, basta multiplicar a matriz inversa de A por cada uma das matrizes-colunas formadas com os blocos codificados e repetir a mesma regra da codificação: cada elemento do produto, maior que 25, deve ser substituído por seu resto na divisão por 26.

Etapa 1: No nosso caso, a inversa será uma matriz quadrada de ordem 2. Logo, da mesma forma como fizemos na codificação, separamos a sequência que representa a mensagem codificada em blocos de tamanho 2 e os escrevemos como matrizes de duas linhas e uma coluna. Assim, como a mensagem codificada é 13-(-11)-20-(-10)-13-(-11)-20-(-2)-3-(-1), temos que os blocos são os seguintes:

$$\begin{bmatrix}13\\-11\end{bmatrix},\begin{bmatrix}20\\-10\end{bmatrix},\begin{bmatrix}13\\-11\end{bmatrix},\begin{bmatrix}20\\-2\end{bmatrix},\begin{bmatrix}3\\-1\end{bmatrix}$$

Etapa 2: Precisamos calcular a inversa da matriz $A=\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}$. Seja $A^{-1}=\begin{bmatrix}x & y\\z & t\end{bmatrix}$ a inversa da matriz A. Pela Definição 4.28, temos que

$$A\cdot A^{-1}=\begin{bmatrix}1 & 0\\-1 & 2\end{bmatrix}\cdot\begin{bmatrix}x & y\\z & t\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$$

Assim, $\begin{bmatrix}1\cdot x+0\cdot z & 1\cdot y+0\cdot t\\(-1)\cdot x+2\cdot z & (-1)\cdot y+2\cdot t\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\Rightarrow\begin{bmatrix}x & y\\-x+2z & -y+2t\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$. Da igualdade de matrizes podemos concluir que

$$x=1, y=0, -x+2z=0 \text{ e } -y+2t=1.$$

Da terceira equação, segue que $2z=x\Rightarrow z=\frac{x}{2}=\frac{1}{2}$. Da mesma forma, da quarta equação, concluímos que $2t=1+y=1+0=1\Rightarrow t=\frac{1}{2}$. Conclusão: $x=1, y=0\ e\ z=t=\frac{1}{2}$. Portanto, $A^{-1}=\begin{bmatrix}1 & 0\\\frac{1}{2} & \frac{1}{2}\end{bmatrix}$.

Etapa 3: Calculada a matriz A^{-1} na Etapa 2, já temos a chave de decodificação. Para decodificar a mensagem

$$\begin{bmatrix}13\\-11\end{bmatrix},\begin{bmatrix}20\\-10\end{bmatrix},\begin{bmatrix}13\\-11\end{bmatrix},\begin{bmatrix}20\\-2\end{bmatrix},\begin{bmatrix}3\\-1\end{bmatrix}$$

devemos decodificar cada um dos blocos que a forma. Para fazer isso, multiplicamos A^{-1} por cada um desses blocos. Assim, pela observação inicial, recuperamos os blocos originais, e o processo está encerrado. A decodificação desses blocos será dada da seguinte forma:

Decodificação do bloco $\begin{bmatrix}\mathbf{13}\\\mathbf{-11}\end{bmatrix}$
Multiplicamos a matriz $\begin{bmatrix}1 & 0\\\frac{1}{2} & \frac{1}{2}\end{bmatrix}$ pela matriz $\begin{bmatrix}13\\-11\end{bmatrix}$. Teremos: $$\begin{bmatrix}1 & 0\\\frac{1}{2} & \frac{1}{2}\end{bmatrix}\cdot\begin{bmatrix}13\\-11\end{bmatrix}=\begin{bmatrix}1\cdot 13+0\cdot(-11)\\\frac{1}{2}\cdot 13+\frac{1}{2}\cdot(-11)\end{bmatrix}=\begin{bmatrix}13+0\\\frac{13}{2}+\frac{-11}{2}\end{bmatrix}=\begin{bmatrix}13\\1\end{bmatrix}$$

Decodificação do bloco $\begin{bmatrix} \mathbf{20} \\ \mathbf{-10} \end{bmatrix}$

Multiplicamos a matriz $\begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ pela matriz $\begin{bmatrix} 20 \\ -10 \end{bmatrix}$. Teremos:

$$\begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 20 \\ -10 \end{bmatrix} = \begin{bmatrix} 1 \cdot 20 + 0 \cdot (-10) \\ \frac{1}{2} \cdot 20 + \frac{1}{2} \cdot (-10) \end{bmatrix} = \begin{bmatrix} 20 + 0 \\ \frac{20}{2} + \frac{-10}{2} \end{bmatrix} = \begin{bmatrix} 20 \\ 5 \end{bmatrix}$$

Decodificação do bloco $\begin{bmatrix} \mathbf{20} \\ \mathbf{-2} \end{bmatrix}$

Multiplicamos a matriz $\begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ pela matriz $\begin{bmatrix} 20 \\ -2 \end{bmatrix}$. Teremos:

$$\begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 20 \\ -2 \end{bmatrix} = \begin{bmatrix} 1 \cdot 20 + 0 \cdot (-2) \\ \frac{1}{2} \cdot 20 + \frac{1}{2} \cdot (-2) \end{bmatrix} = \begin{bmatrix} 20 + 0 \\ \frac{20}{2} + \frac{-2}{2} \end{bmatrix} = \begin{bmatrix} 20 \\ 9 \end{bmatrix}$$

Decodificação do bloco $\begin{bmatrix} \mathbf{3} \\ \mathbf{-1} \end{bmatrix}$

Multiplicamos a matriz $\begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ pela matriz $\begin{bmatrix} 3 \\ -1 \end{bmatrix}$. Teremos:

$$\begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 3 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 \cdot 3 + 0 \cdot (-1) \\ \frac{1}{2} \cdot 3 + \frac{1}{2} \cdot (-1) \end{bmatrix} = \begin{bmatrix} 3 + 0 \\ \frac{3}{2} + \frac{-1}{2} \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$$

O processo de decodificação nos dá a sequência de blocos $\begin{bmatrix} 13 \\ 1 \end{bmatrix}, \begin{bmatrix} 20 \\ 5 \end{bmatrix}, \begin{bmatrix} 13 \\ 1 \end{bmatrix}, \begin{bmatrix} 20 \\ 9 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \end{bmatrix}$. Esta sequência de blocos dá origem a sequência 13-1-20-5-13-1-20-9-3-1 que é a nossa palavra original MATEMÁTICA de acordo com a Tabela 8. Pronto! Recuperamos a mensagem original.

Os roteiros anteriores podem ser usados para quaisquer exemplos utilizando a Cifra de Hill. É claro que o professor está livre para desenvolver o roteiro que achar mais conveniente para trabalhar atividades que envolvam esta cifra em sala de aula. O que propomos é um guia

simples que auxilia na realização dos processos de codificação e decodificação e que deixa claro como os conceitos de matrizes estão inseridos nesses processos.

Na próxima seção continuaremos nosso estudo, agora com foco em probabilidade e sua relação com a criptografia.

4.5 Probabilidade e Criptografia

Nesta seção ampliamos as aplicações da matemática básica a criptografia estudando brevemente a relação entre probabilidade e sigilo perfeito. Como fizemos na Seção 4.4, revisaremos brevemente algumas noções sobre probabilidade, encerrando com uma aplicação em criptografia. Esta relação é mais bem desenvolvida em livros especializados em criptografia, como Terada (2000), Pellegrini (2019) e Buchmann (2002). No entanto, fizemos um genuíno esforço para abordar esse assumo de modo mais simples e didático no contexto da matemática básica.

4.5.1 Noções básicas sobre probabilidade

"Experiências que, repetidas sob as mesmas condições, produzem geralmente resultados diferentes são chamadas de Aleatórias" (LIMA et al., 2006b, p. 82). Assim, por exemplo, experiências como: jogar um dado e observar a face voltada pra cima; jogar uma moeda e observar se deu cara ou coroa; retirar uma bola de uma urna que contêm várias bolas de cores diferentes e observar sua cor; retirar uma carta de um baralho e observar seu nipe; etc., são todas aleatórias.

Nas experiências aleatórias podemos destacar o conjunto de todos os resultados possíveis de ocorrer. Esse conjunto será denotado por S e chamado de Espaço Amostral. Assim, por exemplo, na experiência de retirar uma carta de um baralho comum e observar seu nipe, o Espaço Amostral é {Ouro, Espadas, Paus, Copas}, pois esses são os únicos resultados possíveis da experiência.

Todo subconjunto do Espaço Amostral S será chamado de Evento. "Diremos que um evento ocorre quando o resultado da experiência pertence ao evento" (LIMA et al., 2006b, p. 82). Dentre os eventos de S podemos destacar os eventos chamados triviais, que são o evento

$\emptyset$ (evento nulo ou evento vazio) que nunca ocorre, e o próprio S (evento certo) que sempre ocorre.

Exemplo 4.46 Lança-se um dado normal e observa-se a face voltada para cima. Nesta experiência temos o Espaço Amostral S = {1, 2, 3, 4, 5, 6}. Como o número de subconjuntos de S é $2^6 = 64$, segue que existem 64 eventos possíveis. Dentre eles, podemos destacar os eventos triviais $\emptyset$, S; o evento {2, 4, 6} que ocorre se o resultado da experiência for um número par, e o evento {1, 3, 5} que ocorre quando o resultado da experiência é um número ímpar.

Se considerarmos A e B eventos de S, as operações entre conjuntos nos possibilitará falar dos eventos $A \cup B$, $A \cap B$, $A - B$ e A^c. Quando A e B ocorrem ao mesmo tempo, então $A \cap B$ ocorre. Se ao menos um dos eventos A e B ocorre, então o evento $A \cup B$ ocorre. É fácil ver que o evento $A - B$ só ocorre se A ocorrer e B não. Por fim, A^c ocorre se, e somente se A não ocorrer.

Definição 4.30 Sejam A e B eventos de S. Dizemos que A e B são mutualmente excludentes (ou mutualmente exclusivos) quando eles não ocorrem simultaneamente. Ou seja, $A \cap B = \emptyset$.

Exemplo 4.47 No lançamento de um dado, os eventos A = {2, 4, 6} e B = {1, 3, 5} são mutualmente excludentes.

Definir uma probabilidade (ou uma distribuição de probabilidade) num Espaço Amostral S significa definir uma função $p: S \to \mathbb{R}$. A definição a seguir é baseada na dada por Lima *et al*. (2006b).

Definição 4.31 Uma probabilidade em S é uma função $p: S \to \mathbb{R}$ que faz corresponder a cada evento A de S um número real $p(A) \in \mathbb{R}$, chamado a probabilidade de A, que satisfaz as seguintes condições:

(i) qualquer que seja o evento $A \subset S$, tem-se $0 \leq p(A) \leq 1$;
(ii) a probabilidade do evento certo é 1, isto é, $p(S) = 1$;
(iii) se A e B são eventos mutualmente excludentes, então $p(A \cup B) = p(A) + p(B)$.

Da definição anterior é possível provar facilmente as seguintes propriedades:

- $p(\emptyset) = 0$;
- $p(A^c) = 1 - p(A)$, qualquer que seja o evento $A \subset S$;

- $p(A \cup B) = p(A) + p(B) - p(A \cap B)$, para todos os eventos $A, B \subset S$. Se A e B são eventos quaisquer, temos que $p(A \cap B) = p(A) \cdot p(B/A)$, onde $p(B/A)$ é a probabilidade de B ocorrer sabendo que A ocorreu, e será definida mais adiante. Quando A e B são eventos mutualmente excludentes, temos
$$p(A \cap B) = p(A) \cdot p(B).$$
- Se $A \subset B$, então $p(A) \leq p(B)$.

A prova dessas propriedades podem ser encontradas em Lima *et al*. (2006), ou em qualquer outro livro que trate do assunto.

Para indicar a probabilidade de um evento elementar $a \in S$ usamos a notação $p(a)$, embora o mais correto fosse $p(\{a\})$, apenas por simplicidade de notação. Além disso, para definirmos uma probabilidade em S é suficiente definirmos uma probabilidades sobre seus eventos elementares. Da mesma forma, a probabilidade de um evento A é a soma das probabilidades dos seus eventos elementares.

Exemplo 4.48 Se considerarmos o conjunto das letras do alfabeto usual $\Sigma = \{A, B, C, \dots, Z\}$ e a experiência que consiste em selecionar uma letra desse conjunto para ser codificada por um determinado método criptográfico, então, por exemplo, a probabilidade de escolhermos B (ou resumidamente, a probabilidade de B) será indicada por $p(B)$ ao invés de $p(\{B\})$. Uma probabilidade possível de ser definida em Σ é aquela tal que $p(\emptyset) = 0, p(\Sigma) = 1$ e $p(A) = p(B) = p(C) = \cdots = p(Z) = \frac{1}{26}$ Verifica-se facilmente que todas as condições da definição de probabilidade são satisfeitas.

Definição 4.32 Um Espaço Amostral S será dito equiprovável quando todos os seus eventos elementares tiverem a mesma probabilidade de ocorrer. Equivalentemente, o modelo de probabilidade usado em S é dito equiprobabilístico.

Assim, se S é equiprovável e possui n eventos elementares, então a probabilidade de cada um dos eventos elementares será $\frac{1}{n}$. Com efeito, suponhamos $S = \{a_1, a_2, \dots, a_n\}$. Como a probabilidade de S é a soma das probabilidades dos eventos elementares, segue que:

$$P(S) = P(a_1) + P(a_2) + \cdots + P(a_n).$$

Como $P(a_1) = P(a_2) = \cdots = P(a_n)$, segue que $P(S) = nP(a_n)$. Logo, $P(a_n) = \frac{P(S)}{n} = \frac{1}{n}$. Concluímos assim que a probabilidade de qualquer evento elementar é $\frac{1}{n}$. Disso resulta que se A é um evento de S com x elementos, então

$$P(A) = \frac{x}{n} = \frac{nº\ de\ elementos\ de\ A}{nº\ de\ elementos\ de\ S}.$$

De fato, sendo $A = \{b_1, b_2, \ldots, b_x\}$, temos:

$$P(A) = P(b_1) + P(b_2) + \cdots + P(b_x) = \underbrace{\frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n}}_{x\ parcelas} = \frac{x}{n}.$$

Chegamos assim à famosa fórmula de calcular probabilidades, que assegura que a probabilidade de um evento ocorrer é a razão entre o número de resultados favoráveis ao evento, dividido pelo número de resultados possíveis da experiência. No entanto, é preciso ressaltar, como os cálculos anteriores deixam claro, que essa maneira de pensar no cálculo da probabilidade de um evento A só é válida se o espaço amostral S for equiprovável.

Exemplo 4.49 No experimento que consiste em retirar uma carta de um baralho normal e observar seu nipe, temos que o Espaço amostral é equiprovável, pois consideramos que qualquer nipe tem a mesma chance de ser escolhido. Logo, a probabilidade de sair qualquer nipe é $\frac{1}{4} = 25\%$.

Para encerrar essas considerações sobre probabilidade, abordaremos o importante conceito de *Probabilidade Condicional*. Antes de definirmos esse conceito, vamos resolver um problema que retrata muito bem o significado de probabilidade condicional.

Exemplo 4.50 Numa urna existem 10 bolas idênticas numeradas de 1 à 10. Considere a experiência que consiste em retirar uma bola dessa urna e observar seu número. O Espaço Amostral dessa experiência é S = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}. Se A é o evento {número da bola retirada é par}, isto é, A = {2, 4, 6, 8, 10}, então a probabilidade de A ocorrer é $P(A) = \frac{5}{10} = \frac{1}{2} = 50\%$. Esta é a probabilidade de A ocorrer antes de ser realizada a experiência. Agora, suponhamos que realizada a experiência, tenhamos a informação de que a bola sorteada não foi a de número 5. Pergunta-se: qual a probabilidade de A neste caso? Com a informação de que a bola sorteada não foi a de número 5, a probabilidade de A se modifica. Isso ocorre porque como agora temos a certeza que o evento B = {1, 2, 3, 4, 6, 7, 8, 9, 10}

ocorreu, então temos 9 casos possíveis de ocorrer, sendo que 5 deles são favoráveis. Daí, a probabilidade de A se torna $P(A) = \frac{5}{9} \cong 55{,}5\%$. Assim, podemos dizer que o novo espaço amostral é B, e a probabilidade de A é calculada em B. Assim, o número de casos possíveis passa a ser igual ao número de elementos de B. Da mesma forma, veja que os casos que são favoráveis à ocorrência de A são todos os elementos que pertencem a interseção $A \cap B$. Enfim, dizemos neste caso que $\frac{5}{9}$ é a probabilidade de A na certeza (ou sabendo) que B ocorreu, e escrevemos $P(A\backslash B) = \frac{5}{9}$. Temos então a seguinte definição:

Definição 4.33 Sejam A e B eventos quaisquer de um Espaço Amostral S, com $P(B) \neq 0$. A probabilidade condicional de A ocorrer sabendo que B ocorreu é dada por:

$$P(A\backslash B) = \frac{P(A \cap B)}{P(B)}.$$

Observação 4.6 A justificativa para o uso dessa fórmula no cálculo da probabilidade condicional $P(A\backslash B)$ é bem simples. De fato, como comentamos no Exemplo 4.50, sabendo que B ocorreu, o espaço amostral agora é B. Analogamente, os casos favoráveis não são mais todos os elementos de A, mas sim os elementos de $A \cap B$. Assim:

$$P(A\backslash B) = \frac{nº\ de\ elementos\ de\ A \cap B}{nº\ de\ elementos\ de\ B} = \frac{\frac{nº\ de\ elementos\ de\ A \cap B}{nº\ de\ elementos\ de\ S}}{\frac{nº\ de\ elementos\ de\ B}{nº\ de\ elementos\ de\ S}} = \frac{P(A \cap B)}{P(B)}.$$

A seguir, investigaremos um pouco a relação entre probabilidade e criptografia por meio do conceito de Sigilo Perfeito. Veremos que a abordagem desse conceito também é uma ótima oportunidade para falar de criptografia e probabilidade em sala de aula.

4.5.2 Sigilo Perfeito e Probabilidade

As noções básicas de probabilidade podem ser apreciadas em vários campos da ciência, inclusive em criptografia. O conceito de *Sigilo Perfeito*, tão importante na área de criptografia, é definido com base em probabilidade condicional. A ideia de sigilo perfeito é extremamente simples: suponhamos que um indivíduo A desenvolva um método criptográfico para se comunicar com outro indivíduo B. Um intruso C pretende interceptar a comunicação entre A e B. O indivíduo A codifica uma mensagem (texto comum) x e o manda para B. Supondo que C possa ler a mensagem codificada, o método utilizado por A e B terá sigilo

perfeito se o intruso C nada puder concluir a respeito de x com base no texto cifrado em sua posse (BUCHMANN, 2002). A formulação matemática dessa ideia requer a utilização de probabilidades definidas nos conjuntos (espaços) de texto comum $\mathcal{P}$, texto cifrado $\mathcal{C}$ e de chaves $\mathcal{K}$.

Sendo assim, consideremos um criptossistema onde o espaço de texto comum, o espaço de texto cifrado e o espaço das chaves são finitos. Temos:

(i) Com relação ao conjunto $\mathcal{P}$ podemos considerá-lo como um espaço Amostral. De fato, $\mathcal{P}$ é o espaço amostral da experiência que consiste em escolher um texto comum $x \in \mathcal{P}$. Veja que os eventos elementares desse espaço são os textos comuns x. Portanto, podemos definir uma probabilidade em $\mathcal{P}$, e denotaremos por $p_{\mathcal{P}}(x)$ a probabilidade de x ser escolhido em $\mathcal{P}$.

(ii) Para codificar um texto comum x é preciso de uma chave $k \in \mathcal{K}$. Olhando $\mathcal{K}$ como espaço amostral, a saber, aquele correspondente à experiência que consiste em escolher uma chave para a codificação, cujos eventos elementares são as chaves, definiremos $p_{\mathcal{K}}(k)$ como sendo a probabilidade da chave k ser escolhida. A escolha da chave k não depende de x.

Dados um texto comum x e uma chave $k \in \mathcal{K}$, a probabilidade de x e k serem escolhidos simultaneamente, ou o que é equivalente, a probabilidade de x ser escolhido e a chave de codificação utilizada ser k, é dada por

$$p(\{x\} \cap \{k\}) = p(x) \cdot p(k) = p_{\mathcal{P}}(x) \cdot p_{\mathcal{K}}(k).$$

Onde a probabilidade do texto comum x ser codificado é igual a $p_{\mathcal{P}}(x)$, e denotada por $p(x)$, e a probabilidade de uma chave k ser escolhida para a codificação é $p_{\mathcal{K}}(k)$, denotada por $p(k)$. Por fim, considere o seguinte evento: *codificando x com a chave k obtém-se c*, isto é, $E_k(x) = c$. Veja que este evento é equivalente ao seguinte: *O texto c é o resultado da codificação do texto x*, o qual denotaremos apenas por c. Então, resumidamente, $p(c)$ é a probabilidade de o texto cifrado ser c.

Voltando ao problema do intercâmbio de mensagens de A e B, imaginemos que o intruso C consiga obter um dos textos cifrados c. É de se supor que C conhece a probabilidade definida no espaço $\mathcal{P}$ utilizado por A e B, pois ele pode muito bem conhecer a linguagem utilizada por A e B (BUCHMANN, 2002). Neste caso, C pode usar probabilidade e se fazer a

seguinte pergunta: qual a probabilidade de um texto comum x ter sido escolhido para codificação, sabendo que o texto cifrado correspondente foi c. Ou seja, C está procurando respostas para a probabilidade condicional $p(x/c)$ para os $x \in \mathcal{P}$. Nessa análise, duas possibilidades podem ocorrer: ou C descobre que para determinado x a probabilidade $p(x/c)$ é grande, isto é, há muitas chances de o texto comum correspondente à c ser x, e com isso ele passa a descartar outros textos com probabilidade muito pequena, ou então C não descobre nada com relação aos textos comuns. Isso ocorre quando a probabilidade $p(x/c)$ não fornece nenhuma informação a respeito das chances de x ser o texto comum correspondente a c. Veja que isso ocorre quando os eventos $\{x\}$ e $\{c\}$ são independentes. Nestas condições $p(x/c) = p(x)$.

Buchmann (2002) apresenta uma definição de sigilo perfeito (um caso simples de um resultado mais geral) com base num caso semelhante à segunda possibilidade para C dada anteriormente. Segundo Buchmann (2002), se considerarmos um método criptográfico onde o espaço de chaves é um espaço Amostral equiprovável, e os conjuntos $\mathcal{C}$ e $\mathcal{K}$ tem a mesma quantidade de elementos, então este método terá sigilo perfeito se, e só se $p(x/c) = p(x)$. Um resultado mais geral é conhecido como Teorema de *Shannon* e pode ser encontrado em Buchmann (2002). Para nossos interesses, é suficiente o caso mais simples. Assim, vemos muito facilmente que as probabilidades condicionais são extremamente importantes para a criptografia.

Essa pequena explicação da relação entre probabilidade e sigilo perfeito deve servir como motivação para abordar o assunto dentro do conteúdo de probabilidade. O próximo exemplo é baseado em um exposto em Buchmann (2002).

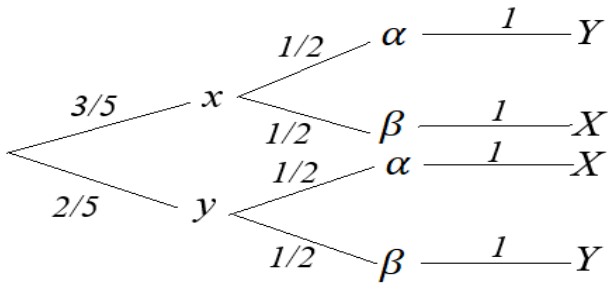
Exemplo 4.51 Digamos que num criptossistema tenhamos $\mathcal{P} = \{x, y\}$, $\mathcal{K} = \{\alpha, \beta\}$ e $\mathcal{C} = \{X, Y\}$. Definamos as seguintes probabilidades:

$$\text{Em } \mathcal{P}\text{: } p(\emptyset) = 0, p(\mathcal{P}) = 1, p(x) = \frac{3}{5} e\ p(y) = \frac{2}{5};$$

$$\text{Em } \mathcal{K}\text{: } p(\emptyset) = 0, p(\mathcal{K}) = 1, p(\alpha) = p(\beta) = \frac{1}{2}.$$

Vamos mostrar que este criptossistema possui sigilo perfeito. Inicialmente, como a função de codificação é uma permutação, ela pode ser definida como $E_\alpha(x) = Y, E_\alpha(y) = X$, $E_\beta(x) = X$ e $E_\beta(y) = Y$. Então, escolhe-se um texto comum, escolhe-se uma chave e efetua-se a codificação. O diagrama de árvore abaixo mostra todas as possibilidades:

Figura 20 – Diagrama de árvore para o problema do Exemplo 4.52



Fonte: Autoria própria

Calculemos as probabilidades $p(x\backslash X), p(x\backslash Y), p(y\backslash Y)$ e $p(y\backslash X)$. Pelo diagrama anterior, esses cálculos ficam muito fáceis. Então, temos:

$$p(x\backslash X) = \frac{p(x \cap X)}{p(X)} = \frac{\frac{3}{5}\cdot\frac{1}{2}}{\frac{3}{5}\cdot\frac{1}{2}+\frac{2}{5}\cdot\frac{1}{2}} = \frac{\frac{3}{10}}{\frac{3}{10}+\frac{2}{10}} = \frac{\frac{3}{10}}{\frac{5}{10}} = \frac{3}{5} = p(x).$$

$$p(x\backslash Y) = \frac{3}{5} = p(x).$$

$$p(y\backslash X) = \frac{p(y \cap X)}{p(X)} = \frac{\frac{2}{5}x\frac{1}{2}}{\frac{2}{5}x\frac{1}{2}+\frac{3}{5}x\frac{1}{2}} = \frac{\frac{2}{10}}{\frac{2}{5}+\frac{3}{5}} = \frac{2}{5} = p(y).$$

$$p(y\backslash Y) = \frac{2}{5} = p(y).$$

As probabilidades acima mostram que o criptossistema em questão possui sigilo perfeito. Veja que se o espaço das chaves não é equiprovável, então o criptossistema não possuirá sigilo perfeito.

Exemplo 4.52 (*One – time Pad de Vernam*) One – time Pad de Vernam é o nome de um método de criptografia, com sigilo perfeito, inventado em 1917 por Gilbert Sandford Vernam (1890 - 1960)[38]. Este método é usado para codificar sequências de n bits em sequências de n bits. Ou seja, ele codifica sequências com n termos, onde cada termo é 1 ou 0, em outra sequência de mesma espécie. O conjunto de todas as sequências de n bits será representado pelo símbolo $\{0,1\}^{(n)}$. Por exemplo, 01011100 é um elemento de $\{0,1\}^{(8)}$. A chave de

[38] Engenheiro americano.

codificação para o One – time Pad de Vernam também é uma sequência de n bits. Escolhido o texto comum $x \in \{0,1\}^{(n)}$ e a chave $k \in \{0,1\}^{(n)}$, o texto cifrado c correspondente a x será obtido por $c = x \oplus k$, sendo $\oplus$ uma operação no conjunto {0, 1} definida segundo a tabela a seguir:

Tabela 16 – Operação com Números Binários

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Fonte: Autoria própria

Dadas duas sequências de n bits, $(x_1, x_2, \dots, x_n)$ e $(y_1, y_2, \dots, y_n)$, definimos $(x_1, x_2, \dots, x_n) \oplus (y_1, y_2, \dots, y_n) = (x_1 \oplus y_1, x_2 \oplus y_2, \dots, x_n \oplus y_n)$. Para decodificar c usamos a mesma fórmula, pois $c \oplus k = (x \oplus k) \oplus k = x \oplus (k \oplus k) = x \oplus 0 = x$, onde 0 representa a sequência nula (0, 0, 0, ..., 0) de $\{0,1\}^{(n)}$. Assim, por exemplo, se $x = 1001010$ *e* $k = 1101100$, então $c = 0100110$.

Na igualdade $c \oplus k = (x \oplus k) \oplus k = x \oplus (k \oplus k) = x \oplus 0 = x$ usamos o fato de que a operação $\oplus$ goza da propriedade associativa, e que o simétrico de qualquer elemento k é ele próprio. Essas propriedades são de verificação imediata. Assim, por exemplo, dado $k \in \{0,1\}^{(n)}$, seja k_i o i-ésimo termo de k. Logo, $k \oplus k$ temo como i-ésimo termo $k_i \oplus k_i$. Sendo que $k_i \in \{0,1\}$, se $k_i = 0$, então $k_i \oplus k_i = 0$. Se $k_i = 1$, então $k_i \oplus k_i = 0$. Portanto, os termos de $k \oplus k$ são todos iguais a zero, isto é, $k \oplus k = 0 = (0, 0, 0, ..., 0)$.

O Exemplo 4.51 está ligado diretamente com o exposto sobre criptografia e probabilidade e, juntamente com a teoria exposta, serve como base motivacional para introduzir o assunto nas discussões sobre as aplicações de probabilidade. Já o Exemplo 4.52 visa apresentar um tipo de criptossistema que possui sigilo perfeito. Para trabalharmos este último exemplo em aulas de matemática, podemos modificar o método apresentado de modo

a torná-lo mais simples. Como sugestão, poderíamos pensar em representar as letras do alfabeto através de sequências de bits distintas, digamos, com 5 bits. Assim, por exemplo, se o P fosse representado por 10010, o A por 01011 e o Z por 11001, poderíamos representar a palavra PAZ como 10010.01011.11001. Usando 11010 como chave de codificação, a palavra PAZ codificada passaria a ser representada por 01000.10001.00010. A codificação do alfabeto pode ser feita usando representação na base 2 (representação binária).

Na prática, trabalha-se com algo semelhante em computação, onde existem os chamados *códigos binários*, que codificam em sequências de bits.[39] Por exemplo, o código ASCII (American Standard Code for Information Interchange) é um tipo especial de código binário que codifica um total de 128 caracteres, entre letras latinas maiúsculas e minúsculas, sinais de pontuação, símbolos matemáticos, etc., em sequências de 7 bits. Nesta sequência de 7 bits que representa cada símbolo, adiciona-se um novo bit para formar uma sequência de 8 bits, que é chamada de byte. Na tabela a seguir, temos uma parte dos símbolos do código ASCII. Para mais informações, consulte as referências dadas em notas de rodapé nesta página.

[39] Conheça mais sobre códigos binários em: <https://pt.wikipedia.org/wiki/Sistema_de_numera%C3%A7%C3%A3o_bin%C3%A1rio#:~:text=O%20sistema%20bin%C3%A1rio%20ou%20de,natural%20%C3%A9%20o%20sistema%20bin%C3%A1rio> e <https://www.portaleducacao.com.br/conteudo/artigos/nutricao/compreendendo-o-codigo-binario/48352 >. Acesso em: 09 jun. 2020.

Tabela 17 – O Código ASCII

Binário	Decimal	Hexa	Glifo
0010 0000	32	20	
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?

Binário	Decimal	Hexa	Glifo
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	[
0101 1100	92	5C	\
0101 1101	93	5D	]
0101 1110	94	5E	^
0101 1111	95	5F	_

Binário	Decimal	Hexa	Glifo
0110 0000	96	60	`
0110 0001	97	61	a
0110 0010	98	62	b
0110 0011	99	63	c
0110 0100	100	64	d
0110 0101	101	65	e
0110 0110	102	66	f
0110 0111	103	67	g
0110 1000	104	68	h
0110 1001	105	69	i
0110 1010	106	6A	j
0110 1011	107	6B	k
0110 1100	108	6C	l
0110 1101	109	6D	m
0110 1110	110	6E	n
0110 1111	111	6F	o
0111 0000	112	70	p
0111 0001	113	71	q
0111 0010	114	72	r
0111 0011	115	73	s
0111 0100	116	74	t
0111 0101	117	75	u
0111 0110	118	76	v
0111 0111	119	77	w
0111 1000	120	78	x
0111 1001	121	79	y
0111 1010	122	7A	z
0111 1011	123	7B	{
0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

Fonte: <http://vamosblablar.blogspot.com/2011/11/tabela-de-codigo-ascii.html>.

Acesso em: 10 jun. 2020

5 CONSIDERAÇÕES FINAIS

Tendo como tema central a Criptografia, o presente trabalho se empenhou em desenvolver e investigar a relação dessa ciência com alguns tópicos de matemática tradicionalmente abordados no ensino básico. Diante do estudo realizado, ficou nítida que a relação entre matemática e criptografia pode ser uma importante aliada do professor nas suas aulas.

A criptografia faz parte da cultura humana desde os tempos mais remotos. Como vimos, com o surgimento da criptografia de chave pública, a matemática passou a ser o pilar de sustentação de toda teoria que assegura confiança e segurança aos métodos criptográficos. Em nível elementar, a teoria que garante a segurança imposta pela criptografia deriva de conceitos simples de matemática que são aprendidos até o fim do Ensino Médio. Portanto, não é difícil falar de criptografia na escola e, mais ainda, de suas aplicações no nosso cotidiano. Ao fazer isso, levamos o aluno a conhecer essa importante inteligência que nos proporciona a segurança necessária nas nossas transações bancárias, comerciais, compras e trocas de mensagens pela internet, etc. Mais fundamental ainda é fazer com que o aluno seja levado a perceber o quão significativa é a matemática para nossa vida. Não é só uma questão de explorar determinados conceitos de matemática em criptografia, e sim educar e situar os estudantes no meio tecnológico e computacional o mais cedo possível.

Nesse sentido, nosso trabalho frisou três pontos principais sobre matemática e criptografia: o contexto histórico, a aritmética básica e o método RSA, e métodos e conceitos elementares de criptografia definidos com base em temas da matemática do Ensino Médio. Tudo isso sempre com a intenção de trabalhar os conteúdos matemáticos dentro do tema criptografia. Isto nos possibilitou ampliar os horizontes de nossa imaginação frente às aplicações da matemática, pois a priori é difícil de imaginar como determinados temas, como Probabilidades, por exemplo, estejam relacionados com algo como criptografia. Essa relação inesperada entre determinados conteúdos de matemática e criptografia torna-se elemento fundamental de inspiração, motivação e atração nas aulas de matemática.

Para que nossos objetivos fossem alcançados e essa relação entre matemática básica e criptografia fosse desenvolvida da melhor forma possível de acordo com os propósitos deste trabalho, foi necessário desenvolver o tema de modo que o leitor (principalmente o professor) tivesse condições de introduzir a criptografia e tratá-la nos vários níveis da educação básica.

Assim, numa excursão ao presente trabalho, iniciamos conhecendo um pouco da história da criptografia (é sempre bom começar um tema novo em nossas aulas tratando da sua história), como a mesma surgiu e como se desenvolveu ao longo do tempo. Neste caso, ao analisarmos a história da criptografia, também aprendemos os conceitos básicos e alguns dos métodos clássicos dessa ciência. Sem contar que é por meio da história que passamos a entender melhor porque a criptografia foi criada e porque ela foi responsável por enormes avanços na tecnologia das comunicações. De épocas de grandes Reis e Rainhas, passando pelas grandes Guerras Mundiais, até a modernidade da internet, a criptografia sempre foi o assunto dominante quando se tratava do sigilo nos envios de mensagens, sendo personagem principal de vários episódios marcantes na história da humanidade. É sem dúvidas uma ótima ideia começar a falar de criptografia a partir de sua história.

A aritmética básica surge em seguida no nosso estudo como requisito obrigatório para entender a funcionalidade de um dos métodos de criptografia mais importantes na atualidade, o RSA. Sem precisar expandir o estudo da Teoria Elementar dos Números, nos preocupamos em apenas frisar aqueles conceitos mais importantes para o entendimento do RSA. Desta forma, concluímos que muitos dos conceitos necessários para a compreensão do método RSA derivam de noções simples que aprendemos desde cedo na escola, como Divisibilidade, Números Primos e Máximo Divisor Comum. Assim sendo, é possível tratar a relação entre aritmética básica e criptografia sem ter um conhecimento avançado em matemática. Ou seja, como deixamos claro no trabalho, é possível levarmos a discussão sobre criptografia e matemática também para o ensino fundamental. Melhor ainda é o fato de que boa parte do que expomos neste trabalho pode ser aplicado nesta fase do ensino, com algumas modificações. Conclui-se então que criptografia e matemática também pode ser tema a ser bem trabalhado nas aulas de matemática no ensino fundamental, expandindo ainda mais as utilidades dessa relação no ensino.

Finalizamos o nosso trabalho tratando de desenvolver o nosso objetivo principal que buscou relacionar determinados tópicos de matemática do Ensino Médio com a criptografia. Vimos que assuntos como Matrizes, Funções Afins, Funções Quadráticas e Probabilidades são tópicos que aparecem com muita frequência nos estudos sobre criptografia. Destacamos esses tópicos, entre outros, e passamos a investigar conceitos e métodos criptográficos com base nos mesmos. Isso fez com que surgissem as relações, e aplicações, dos conteúdos matemáticos na criptografia. Passamos então a explorar essas relações buscando deixar

evidente de que forma o conteúdo em questão podia ser relacionado, em particular com o método criptográfico em questão.

Desse modo, como mais um auxílio para o professor em sala de aula, desenvolvemos em algumas seções roteiros relacionados à aplicação de determinados métodos criptográficos na codificação de mensagens. Tais roteiros funcionam como guias para a aplicação de atividades envolvendo criptografia. No Capítulo 3 esse guia constitui-se dos Algoritmos 3.1 e 3.2 que ensinam, passo a passo, o funcionamento do método RSA e, portanto, pode ser utilizado para trabalhar este método com os alunos. No Capítulo 4 desenvolvemos guias para a utilização de métodos criptográficos relacionados a funções afins e quadráticas, Seções 4.2.1 e 4.3.1, e matrizes, Seção 4.4.2. De modo geral, fica claro que as relações apresentadas e os exemplos dados funcionarão como fonte principal de atividades (essa é a intenção) que serão elaboradas pelo próprio professor (e de acordo com o nível e experiência de cada turma) em sala de aula. Entretanto, é preciso destacar que tais atividades só serão bem confeccionadas e aplicadas se o professor estiver disposto a adentrar e estudar o tema criptografia e matemática na temática proposta por esse trabalho e nos trabalhos dados nas referências. Só assim ele será capaz de extrair essas aplicações do texto e agregá-las a suas aulas.

Assim, deste breve estudo sobre matemática e criptografia, fica a certeza de que a criptografia é um tema inovador em sala de aula (apesar de ser uma ciência bem antiga) que, corretamente tratado, fornece ao professor uma ferramenta poderosíssima para melhorar a qualidade do ensino e aprendizagem em matemática, tornando suas aulas mais criativas, atrativas, com mais rendimentos e mais próxima da realidade do aluno. Os benefícios para o aluno são inúmeros. Podemos inclui, entre outras coisas, o desenvolvimento do seu raciocínio lógico-dedutivo e de suas habilidades de resolução de problemas. Sem contar que trabalhar o tema criptografia na educação básica fornece uma ótima oportunidade para que o aluno possa ser inserido no campo dessas ciências que dominam a tecnologia da computação.

Ao concluir um trabalho desta magnitude, esperamos acima de tudo que o mesmo seja útil. Em outras palavras, esperamos que o exposto aqui sirva de suporte para o professor para os fins a que foi destinado e que isto reflita em melhorias para o ensino de matemática, que é o nosso propósito. Caso contrário, de nada valeu tudo isso. Portanto, esperamos que este estudo abra um leque de possibilidades e sirva de base motivacional e conceitual para o desenvolvimento de outros trabalhos que tratem de buscar novas estratégias para a melhoria do ensino de matemática por meio da criptografia. E, reiterando, tudo isso só será bem

desenvolvido (e com bons resultados) se estivermos dispostos a encarar as dificuldades e procurar sempre estudar e explorar o tema em busca de elementos que possam apontar caminhos para a criação de estratégias para abordar a criptografia em sala de aula. De outra forma, essas ideias ficarão apenas no papel.

Como sugestão para trabalhos futuros, podemos destacar algumas ideias que certamente seriam bem vindas em sala de aula. No ensino fundamental pode-se facilmente trabalhar a história da criptografa como forma de inserir os alunos nesse nosso tema. Animações em slides; confecções de dispositivos clássicos de criptografia; leituras de relatos históricos envolvendo trocas secretas de mensagens (como a história de Maria, a rainha da Escócia, veja Singh (2004)); utilização de filmes com o tema criptografia; trabalhos com cifras primitivas; etc., tudo isso leva o aluno a perceber a importância da criptografia no passado e no presente e como a matemática ajudou no desenvolvimento de métodos cada vez mais seguros de codificação. As atividades envolvendo cifras clássicas e métodos primitivos de criptografia são ótimas alternativas para explicar, na prática, como os mesmos funcionavam.

No ensino médio, o presente estudo já dá inúmeras sugestões de trabalhos a serem realizados com o tema criptografia. Como sugestão para testar o funcionamento dos métodos criptográficos na prática, pode-se pensar na implementação de alguns deles, na forma de algoritmos, em alguma linguagem de programação. Por exemplo, o RSA, por meio dos Algoritmos 3.1 e 3.2 pode ser implementado e com isso o aluno pode utilizá-lo na prática para codificar mensagens. Não é algo simples, pois se trata do RSA, principal sistema de criptografia utilizado hoje em dia, mas já existem muitas referências de como fazer isso, e o professor de matemática, com ajuda de um profissional da computação, pode levar facilmente o RSA para a sala de aula.

REFERÊNCIAS

ALENCAR FILHO, Edgard de. **Teoria Elementar dos Números**. 3ª ed. São Paulo: Nobel, 1989.

ALENCAR FILHO, Edgard de. **Teoria Elementar dos Conjuntos**. 13ª ed. São Paulo: Nobel, 1972.

BRANDÃO, Mariana Martins Durões. **Uma Adaptação da Cifra de Hill para Estudo de Matrizes**. 91f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade Federal de Ouro Preto, Ouro Preto/MG, 2017.

BALESTRI, Rodrigo. **Matemática 1:** Interação e Tecnologia. 2ª ed. São Paulo: LEYA, 2016.

BUCHMANN, Johannes A. **Introdução à Criptografia**. 1ª ed. São Paulo: BERKELEY, 2002.

BESSELAAR, Jose' Van Den. **Heródoto, o pai da história**. V. 24, n. 49, Jan./mar. 1962. (4 - 26).

BIANCHINI, Edwaldo. **Matemática Bianchini**, 9º ano. 9ª ed. São Paulo: MODERNA, 2018.

BRASIL, Ministério da Educação. Secretaria de Educação Especial. **Grafia Braille para a Língua Portuguesa**. Brasília, DF: SEESP, 2006.

BROUSSEAU, Guy. **Fondement et Méthodes de la Didactique des Mathématiques**. In J. Brun (Ed), Didactique des Mathématiques, p. 45 – 144. Lausanne: Delachaux et Niestlê, 1996. Citado por PINHEIRO, Felipa Margarida Dias Lima. **Contextualização do Saber: Formação Inicial dos Professores de 1º e 2º Ciclo do Ensino Básico**. 159f. Dissertação (Mestrado em Ciências da Educação), Universidade de Lisboa, Instituto de Educação, Lisboa, 2012.

BROOKSHEAR, J. Glenn. **Ciência da Computação: uma visão abrangente**. 11ª ed. Porto Alegre: BOOKMAN, 2013.

BRASIL. **Base Nacional Comum Curricular: Ensino Médio**. Brasília: MEC/Secretaria de Educação Básica, 2017.

CARNEIRO, Framilson José Ferreira. **Criptografia e Teoria dos Números**. 1ª ed. Rio de Janeiro: CIÊNCIA MODERNA, 2017.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. 2ª ed. Rio de Janeiro: IMPA, 2005.

COUTINHO, S. C. **Criptografia**. Programa de Iniciação Científica da OBMEP. 1ª ed. Rio de Janeiro: IMPA/OBMEP, 2009.

COSTA, Renata. Como funciona o código Braille? **Nova Escola**, 2009. Disponível em: <https://novaescola.org.br/conteudo/397/como-funciona-sistema-braille>. Acesso em: 19 out. 2019.

DANTE, Luiz Roberto. **Matemática**, 1ª série. 1ª ed. São Paulo: Ática, 2006.

DANTE, Luiz Roberto. **Matemática**, volume único. 1ª ed. São Paulo: Ática, 2011.

DAINEZE, Kelly Cristina Santos Alexandre de Lima. **Números Primos e Criptografia**: da relação com a educação ao sistema RSA. 56f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade Federal Rural do Rio de Janeiro, Seropédica/RJ, 2013.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática**, 2010. 161f. Dissertação (Mestrado em Matemática para Professores) – Faculdade de Ciências – Universidade de Lisboa, Lisboa, 2010.

FREITAS, Rosiane de. *et al*. Cifra de César – **Princípios de criptografia como trote educacional e em comemoração ao dia da mulher**. Disponível em: <http://cleilaclo2018.mackenzie.br/docs/LAWCC/188504.pdf>. Acesso em: 10 set. 2019.

FRANÇA, Waldizar Borges de Araújo. **A utilização da Criptografia para uma Aprendizagem Contextualizada e Significativa**. 63f. Dissertação (Mestrado Profissional em Matemática), Universidade de Brasília - UNB, Brasília, 2014.

FRANCISCO, Wagner de Cerqueria e. Código Morse. **Brasil Escola**, 2019. Disponível em: <https://brasilescola.uol.com.br/geografia/codigo-morse.htm>. Acesso em 29 out. 2019.

GIOVANNI JÚNIO, José Ruy; CASTRUCCI, Benedicto. **A Conquista da Matemática**, 9º ano. 4ª ed. São Paulo: FTD, 2018.

HOWARD, Anton; RORRES, Chris. **Álgebra linear com aplicações**. 8 ed. Porto Alegre: Bookman, 2001.

HEFEZ, Abramo. **Curso de Álgebra, vol. 1**. 5ª ed. Rio de Janeiro: IMPA, 2014.

IEZZI, Gelson; DOLCE, Osvaldo; DEGENSZAJN, David; PÉRIGO, Roberto. **Matemática**, volume único. 1ª ed. São Paulo: ATUAL, 2002.

IEZZI, Gelson; HAZZAN, Samuel. **Fundamentos de Matemática Elementar**, vol.4. 7ª ed. São Paulo: ATUAL, 1993.

JULIO, Eduardo Pagani; BRAZIL, Wagner Gaspar; ALBUQUERQUE, Célio Vinicius Neves. Esteganografia e Suas Aplicações. *In*: . **VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais: Livro Texto dos Minicursos.** Brasília, DF: Sociedade Brasileira de Computação – SBC, 2007. p. 54 – 102.

JESUS, André Luís Neris de. **Criptografia na Educação Básica**: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes. 82f. Dissertação

(Mestrado Profissional em Rede Nacional em Matemática - PROFMAT), Universidade Federal do Vale do São Francisco, Juazeiro/BH, 2013.

LIMA, Elon Lages; CARVALHO, Paulo Cezar Pinto; WAGNER, Eduardo; MORGADO, Augusto César. **A Matemática do Ensino Médio, vol. 1**. 9ª ed. Rio de Janeiro: SBM, 2006.

LIMA, Elon Lages; CARVALHO, Paulo Cezar Pinto; WAGNER, Eduardo; MORGADO, Augusto César. **A Matemática do Ensino Médio, vol. 2**. 6ª ed. Rio de Janeiro: SBM, 2006.

LIMA, Elon Lages. **Curso de Análise, vol. 1**. 14ª ed. Rio de Janeiro: IMPA, 2013.

LOUREIRO, Flávio Ornellas. **Tópicos de Criptografia para o Ensino Médio.** 43f. Dissertação (Mestrado em Matemática) Universidade Estadual do Norte Fluminense Darcy Ribeiro – UENF. Campos dos Goytacazes/RJ, 2014.

MALAGUTTI, Pedro Luiz. **Atividade de Contagem a Partir da Criptografia**. Rio de Janeiro: IMPA, 2015.

MEDEIROS, Willa da Silva. **Números Primos e Criptografia RSA**: uma descrição da mais bela relação em teoria dos números. 70f. Monografia (Licenciatura Plena em Matemática), Universidade do Estado do Rio Grande do Norte – UERN. Patu/RN, 2017.

MARTINEZ, Fábio Brochero; MOREIRA, Carlos Gustavo; SALDANHA, Nicolau; TENGAN, Eduardo. **Teoria dos Números**: um passeio com primos e outros números familiares pelo mundo inteiro. 2ª ed. Rio de Janeiro: IMPA, 2013.

MONTEIRO, Luiz H. Jacy. **Elementos de Álgebra**. Rio de Janeiro: AO LIVRO TÉCNICO, 1969.

PORTO, Gabriella. Código Morse. **Info Escola**, [entre 2006 e 2019]. Disponível em: < https://www.infoescola.com/comunicacao/codigo-morse/>. Acesso em: 19 out. 2019.

PELLEGRINI, Gerônimo. **Introdução à Criptografia e seus Fundamentos**, 29 de nov. de 2019. 411f. Notas de aula.

PEREIRA, Nádia Marques Ikeda**. Criptografia: uma nova proposta de ensino de matemática no ciclo básico**. 76f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade Estadual Paulista "Júlio de Mesquita Filho", Ilha Solteira/SP, 2015.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos Números**. 3ª ed. Rio de Janeiro: IMPA, 2014.

SOUSA, Lana Priscila. **Criptografia RSA**: A teoria dos números posta em prática. 75f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade Federal do Ceará, Fortaleza/CE, 2015.

SPINA, André Vinícius. **Números primos e criptografia**. 52f. Dissertação (Mestrado em Matemática), Universidade Estadual de Campinas, São Paulo, 2014.

OKUMURA, Mirella Kiyo. **Números Primos e Criptografia RSA**. 54f. Dissertação (Programa de Mestrado Profissional em Matemática), Instituto de Ciências Matemática e de Computação – ICMC, Universidade de São Paulo, São Paulo/SP, 2014.

SAUTOY, Marcus Du. **A música dos números primos**: a história de um problema não resolvido na matemática. Rio de Janeiro: ZAHAR, 2007.

SHOKRANIAN, Salahoddin. **Criptografia Para Iniciantes**. Brasília: UNB, 2005.

SINGH, Simon. **O livro dos códigos**. 4ª ed. Rio de Janeiro: Record, 2004.

TERADA, Routo. **Segurança de Dados**: criptografia em redes de computador. São Paulo: EDGARD BLÜCHER LTDA, 2000.

TAVARES, Naiara Pereira; FELIX, Francisca Edna Ferreira; GONÇALVES, Maria Cassiana Pereira; CORDEIRO JUNIOR, Reginaldo Amaral. **Criptografia**: uma ferramenta de ensino das operações matriciais. *In*: IV CONGRESSO NACIONAL DE EDUCAÇÃO, 2017, João Pessoa/PB. **Anais**... João Pessoa/PB: REALIZE, 2017.