UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE MESTRADO PROFISSIONAL
EM ENSINO DE CIÊNCIAS EXATAS

PEDRO VALIM SAMPAIO

CRIPTOGRAFIA EM UMA ABORDAGEM ELEMENTAR

SÃO CARLOS
2021

PEDRO VALIM SAMPAIO

CRIPTOGRAFIA EM UMA ABORDAGEM ELEMENTAR

Dissertação apresentada ao Programa de Pós-Graduação em Ensino de Ciências Exatas como requisito parcial para a obtenção do grau de Mestre.

Orientador: Prof. Dr. Wladimir Seixas

SÃO CARLOS
2021

Valim Sampaio, Pedro

Criptografia Em Uma Abordagem Elementar / Pedro Valim Sampaio -- 2021.
72f.

Dissertação (Mestrado) - Universidade Federal de São Carlos, campus São Carlos, São Carlos
Orientador (a): Wladimir Seixas
Banca Examinadora: Wladimir Seixas, Carina Alves Severo, Jose Antonio Salvador
Bibliografia

1. Ensino de Matemática. 2. Criptografia Elementar. 3. Criptografia RSA. I. Valim Sampaio, Pedro. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Ronildo Santos Prado - CRB/8 7325

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Ensino de Ciências Exatas

Folha de Aprovação

Defesa de Dissertação de Mestrado do candidato Pedro Valim Sampaio, realizada em 05/08/2021.

Comissão Julgadora:

Prof. Dr. Wladimir Seixas (UFSCar)

Profa. Dra. Carina Alves Severo (UNESP)

Prof. Dr. Jose Antonio Salvador (UFSCar)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.
O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Ensino de Ciências Exatas.

Dedico este trabalho aos meus pais e a todas as pessoas que, através da educação e do amor, dedicam-se a tornar o mundo um lugar mais justo.

AGRADECIMENTOS

Agradeço primeiramente ao Prof. Dr. Wladimir Seixas, pela confiança em mim depositada ao assumir a orientação deste trabalho. Agradeço também a meu pai Prof. Dr. João Carlos Vieira Sampaio pela coorientação deste trabalho;

À minha mãe Elsa Machado Valim Sampaio, minha irmã Joana Valim Sampaio, meu primo Thiago Ferreira Valins, meu cunhado Ícaro Santiago Martins, meu sobrinho Samael Sampaio Martins;

A todos os professores, alunos colegas de turma e funcionários do PPGECE da UFSCar.

É fazendo que se aprende a fazer aquilo que se deve aprender a fazer.

Aristóteles

RESUMO

Este trabalho apresenta de maneira sucinta aspectos históricos e matemáticos de criptografias antigas e modernas tais como cifra de César, cifras afins, cifra de Vigenère, cifra de Hill e criptografia RSA. São buscados na BNCC e nos PCN-EM orientações sobre o tema de criptografia e atividades relacionadas no ensino médio. No trabalho é feito um desenvolvimento de requisitos matemáticos a uma compreensão elementar dos sistemas criptográficos estudados. Dentre esses requisitos temos conceitos elementares como matrizes, aritmética modular e teoria dos números, os quais são utilizados nas teorias de criptografias apresentadas. Algumas atividades para o professor do ensino básico aplicar em suas aulas são sugeridas ao final.

Palavras-chave: Ensino de Matemática. Criptografia Elementar. Criptografia RSA.

ABSTRACT

This work succinctly presents historical and mathematical aspects of ancient and modern cryptography such as Caesar cipher, related ciphers, Vigenère cipher, Hill cipher and RSA cryptography. Guidance on the subject of cryptography and related activities in high school is sought at the BNCC and PCN-EM. The work develops mathematical requirements for an elementary understanding of the cryptographic systems studied. Among these requirements we have elementary concepts such as matrices, modular arithmetic and number theory, which are used in the presented cryptography theories. Some activities for the elementary school teacher to apply in their classes are suggested at the end.

Keywords: Mathematics Teaching. Elementary Cryptography. RSA Cryptography.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Esta dissertação deveria ter sido sobre a concepção, aplicação, coleta de dados e conclusões sobre uma atividade de aulas inéditas em uma sala de aula do Ensino Médio.

No entanto, o autor, enquanto professor temporário em uma escola estadual da cidade de São Carlos, viu suas intenções completamente desfeitas pela pandemia que assolou nosso país desde março de 2020. As aulas de 2020, tendo sido desfeitas no modo presencial a partir do mês de março, ao longo do ano tiveram a intervenção do professor apenas na proposição e correção de tarefas que eram sugeridas sobre os temas de matemática desenvolvidos em vídeo-aulas pela Secretaria de Educação do Estado de São Paulo.

Entrando 2021 com a pandemia ainda fora de controle e o ensino substancialmente não presencial, viu-se o autor fora do sistema de ensino a partir de fevereiro de 2021. Assim surgiu a ideia de um estudo de elementos históricos e matemáticos de criptografia, da maneira mais elementar possível, de modo que alguns dos tópicos estudados pudessem sugerir atividades para aulas diferenciadas no ensino médio e nas séries finais do ensino fundamental.

O material fascinante encontrado nesses estudos deram origem ao texto desta dissertação.

Na organização do texto, o Capítulo 2 busca, embora sucintamente, estabelecer as relações entre criptografia e a Base Nacional Comum Curricular e os Parâmetros Nacionais Curriculares-Ensino Médio.

No Capítulo 3 são trabalhados pré-requisitos matemáticos para a compreensão de sistemas de Criptografia, que envolvem matrizes, teoria dos números e aritmética modular.

O Capítulo 4 tem como apoio os conceitos do Capítulo 3 em aplicações para desenvolvimento dos algoritmos de criptografia como Cifra de César, Cifra afim, Cifra de Vigenère, Cifra de Hill e Criptografia RSA.

No Capítulo 5 algumas atividades para o professor do ensino básico aplicar em sala de aula são apresentadas.

O autor licenciou-se em Matemática pela Universidade Federal de São Carlos em 2009, foi professor de escola privada do ensino médio no ano de 2011, e em escolas estaduais de São Carlos no período 2013–2014 e 2020–2021. Concluiu um mestrado profissionalizante na Universidade Estadual Paulista, IGCE–Campus de Rio Claro em dezembro 2017. Ocupou também o cargo de professor substituto no Departamento de Matemática da UFSCar no período março de 2012 a julho de 2013.

É estudante do Programa de Pós-Graduação em Ensino de Ciências Exatas da Universidade Federal de São Carlos desde agosto de 2018.

2 A BNCC E OS PCN-EM

A Base Nacional Comum Curricular (BNCC) é atualmente um guia para nortear as ações de professores em suas atividades de ensino. Ali não há menção à exploração de atividades que envolvam criptografia e sua matemática. No entanto, já nas considerações sobre o ensino fundamental, encontramos

> As competências que estão diretamente associadas a representar pressupõem a elaboração de registros para evocar um objeto matemático. Apesar de essa ação não ser exclusiva da Matemática, uma vez que todas as áreas têm seus processos de representação, em especial nessa área é possível verificar de forma inequívoca a importância das representações para a compreensão de fatos, ideias e conceitos, uma vez que o acesso aos objetos matemáticos se dá por meio delas. Nesse sentido, na Matemática, o uso dos registros de representação e das diferentes linguagens é, muitas vezes, necessário para a compreensão, a resolução e a comunicação de resultados de uma atividade. Por esse motivo, espera-se que os estudantes conheçam diversos registros de representação e possam mobilizá-los para modelar situações diversas por meio da linguagem específica da matemática – verificando que os recursos dessa linguagem são mais apropriados e seguros na busca de soluções e respostas – e, ao mesmo tempo, promover o desenvolvimento de seu próprio raciocínio.

Dentre as competências matemáticas para o ensino médio, preconizadas pela BNCC, na seção Competência Específica 4, subtítulo *Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas.* (BNCC, 2020, p. 538), encontramos

> . . . para as aprendizagens dos conceitos e procedimentos matemáticos, é fundamental que os estudantes sejam estimulados a explorar mais de um registro de representação sempre que possível. Eles precisam escolher as representações mais convenientes a cada situação, convertendo-as sempre que necessário. A conversão de um registro para outro nem sempre é simples, apesar de, muitas vezes, ser necessária para uma adequada compreensão do objeto matemático em questão, pois uma representação pode facilitar a compreensão de um aspecto que outra não favorece.

Na seção *5.2.1.1. CONSIDERAÇÕES SOBRE A ORGANIZAÇÃO CURRICULAR* encontramos como competência a ser desenvolvida na unidade NÚMEROS E ÁLGEBRA (BNCC, 2020, p. 543-544),

> (EM13MAT302) Construir modelos empregando as funções polinomiais de 1° ou 2° graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais.
>
> (EM13MAT507) Identificar e associar progressões aritméticas (PA) a funções afins de domínios discretos, para análise de propriedades, dedução de algumas fórmulas e resolução de problemas.

Nesse contexto, considera o autor oportuna a ideia de introduzir conceitos de criptografia elementar como tema de matemática que pode ser explorado nas séries finais do ensino fundamental e na matemática do ensino médio quando se desenvolve a exploração do conceito de função.

Criptografia é, em certa medida, um conceito que envolve a aplicação de uma função que associa cada mensagem a ser codificada a um código que precisa ser decodificado por uma função inversa.

Em uma primeira exploração de criptografia, as funções envolvidas são de natureza elementar. Os modelos matemáticos empregados para descrever a chamada *cifra de César*, ou sua generalização na forma de *cifras afins* envolvem funções afins, bem como também uma aritmética modular elementar, como a do relógio analógico das 24 horas, em que podemos convencionar que, em se tratando de horas, $22 + 5 = 3$. Dizemos que uma tal aritmética é uma aritmética de inteiros *módulo* 24, em que identificamos $24 = 0$. Nas cifras afins e nas cifras de Hill adotamos uma aritmética módulo 26, número das letras do alfabeto latino.

A exploração das *cifras de Hill* é um excelente recurso para explorar a álgebra das matrizes, tão carente na matemática do ensino médio nos dias atuais (opinião do autor). Além de matrizes, 2×2 a princípio, também fazemos uso de uma aritmética modular módulo 26.

Para encerrar este capítulo, mencionamos uma observação pedagógica sobre o ensino de matemática no ensino médio, contida no documento Parâmetros Nacionais Curriculares – Ensino Médio, de 1998 (PCN-EM, 1998).

> A unidade temática Álgebra, por sua vez, tem como finalidade o desenvolvimento de um tipo especial de pensamento – pensamento algébrico – que é essencial para utilizar modelos matemáticos na compreensão, representação e análise de relações quantitativas de grandezas e, também, de situações e estruturas matemáticas, fazendo uso de letras e outros símbolos. Para esse desenvolvimento, é necessário que os alunos identifiquem regularidades e padrões de sequências numéricas e não numéricas, estabeleçam leis matemáticas que expressem a relação de interdependência entre grandezas em diferentes contextos, bem como criar, interpretar e transitar entre as diversas representações gráficas e simbólicas, para resolver problemas por meio de equações e inequações, com compreensão dos procedimentos utilizados.

Acreditamos que, embora de maneira não explícita, os PCN-EM enfatizam a importância da exploração, em atividades de ensino, de uma ferramenta como a criptografia para o ensino de conceitos básicos de matemática do ensino médio.

3 PRELIMINARES MATEMÁTICOS

Neste capítulo são desenvolvidos conceitos matemáticos que o autor considera relevantes para uma compreensão adequada de criptografia elementar. Os conceitos apresentados foram organizados à medida que o autor sentia necessidade de apresentá-los como requisitos à leitura do capítulo sobre criptografia.

3.1 MATRIZES E OPERAÇÕES MATRICIAIS

A álgebra elementar de matrizes é parte importante da formação matemática de estudantes do ensino médio. Também é uma ferramenta usada na definição do sistema de criptografia denominado *cifras de Hill*. Esta seção trata de uma revisão da álgebra elementar de matrizes. Para a construção desta seção, fizemos uso de definições e resultados, bem como de notações, de (ANTON; RORRES, 2012).

Definição 3.1. Uma **matriz** é um agrupamento de números reais em linhas e colunas, de forma retangular. Dizemos que os números nesse agrupamento são as entradas da matriz.

Exemplo 3.1. Alguns exemplos de matrizes são

$$\begin{pmatrix} 1 & 2 & 4 \\ 0 & 7 & 9 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 4 \\ 0 & 7 & 9 \\ 3 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 13 \\ 7 \end{pmatrix}, \quad \begin{pmatrix} 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 2 \end{pmatrix}.$$

O **tamanho** de uma matriz é descrito em termos do número de linhas (fileiras horizontais) e de colunas (fileiras verticais) que ela contém.

Por exemplo, a primeira matriz do Exemplo 3.1 tem duas linhas e três colunas, portanto, seu tamanho é 2 por 3 (e escrevemos 2×3). As outras matrizes do Exemplo 3.1 têm tamanhos 3×3, 2×1, 1×2, 1×1, respectivamente.

Numa descrição de tamanho, o primeiro número sempre denota o número de linhas e o segundo, o de colunas.

Uma matriz com somente uma coluna é denominada **matriz coluna**, ou **vetor coluna**, e uma matriz com somente uma linha é denominada **matriz linha**, ou **vetor linha**.

Quando discutimos matrizes, é costume dizer que as quantidades numéricas são **escalares**. Salvo menção explícita em contrário, escalares são números reais.

A entrada que ocorre na linha i e coluna j de uma matriz A, pode ser denotada por

a_{ij}. Assim uma matriz arbitrária 2×2 pode ser escrita como

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

e uma matriz arbitrária $m \times n$ pode ser denotada como

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Quando for desejada uma notação mais compacta, a matriz precedente pode ser escrita como $[a_{ij}]_{m\times n}$ ou $[a_{ij}]$.

Vetores linha e coluna são de importância especial, e é prática comum denotá-los por letras minúsculas em negrito em vez de letras maiúsculas. Para tais matrizes, é desnecessário usar índices duplos para as entradas. Um vetor linha $1 \times n$ arbitrário **a** e um vetor coluna $m \times 1$ arbitrário **b** podem ser escritos como

$$\mathbf{a} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \end{pmatrix}, \qquad \mathbf{b} = \begin{pmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{m1} \end{pmatrix}.$$

Dizemos que uma matriz A com n linhas e n colunas é uma **matriz quadrada de ordem n**, e que as entradas $a_{11}, a_{22}, \ldots, a_{nn}$ constituem a **diagonal principal** de A.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

Definição 3.2. Duas matrizes são definidas como sendo **iguais** se tiverem o mesmo tamanho e suas entradas correspondentes forem iguais.

A igualdade de duas matrizes $A = [a_{ij}]$ e $B = [b_{ij}]$ de mesmo tamanho pode ser expressa escrevendo $(A)_{ij} = (B)_{ij}$ ou, então, $a_{ij} = b_{ij}$ entendendo-se que as igualdades são válidas para quaisquer valores de i e j.

Definição 3.3. Se A e B são matrizes de mesmo tamanho, então a soma $A + B$ é a matriz

obtida somando as entradas de B às entradas correspondentes de A, e a diferença $A - B$ é a matriz obtida subtraindo as entradas de B das entradas correspondentes de A. Matrizes de tamanhos distintos não podem ser somadas ou subtraídas.

Em notação matricial, se $A = [a_{ij}]$ e $B = [b_{ij}]$ têm o mesmo tamanho, então

$$(A + B)_{ij} = (A)_{ij} + (B)_{ij} = a_{ij} + b_{ij}, \qquad (A - B)_{ij} = (A)_{ij} - (B)_{ij} = a_{ij} - b_{ij}.$$

Definição 3.4. Se A for uma matriz e α um escalar, então o produto αA é a matriz obtida pela multiplicação de cada entrada da matriz A por α. Dizemos que a matriz αA é um múltiplo escalar de A.

Em notação matricial, se $A = [a_{ij}]$, então

$$(\alpha A)_{ij} = \alpha(A)_{ij} = \alpha a_{ij}.$$

Definição 3.5. Se A for uma matriz $m \times r$ e B uma matriz $r \times n$, então o produto AB é a matriz $m \times n$ cujas entradas são determinadas como segue. Para obter a entrada na linha i e coluna j de AB, destacamos a linha i de A e a coluna j de B. Multiplicamos as entradas correspondentes da linha e da coluna e então somamos os produtos resultantes.

Exemplo 3.2. Multiplicação de matrizes

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 & 5 \\ 0 & 7 & 9 & 6 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 0 & 1 \cdot 2 + 2 \cdot 7 & 1 \cdot 4 + 2 \cdot 9 & 1 \cdot 5 + 2 \cdot 6 \\ 0 \cdot 1 + 3 \cdot 0 & 0 \cdot 2 + 3 \cdot 7 & 0 \cdot 5 + 3 \cdot 9 & 0 \cdot 5 + 3 \cdot 6 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 16 & 22 & 17 \\ 0 & 21 & 27 & 18 \end{pmatrix}.$$

A definição de multiplicação de matrizes exige que o número de colunas do primeiro fator A seja igual ao número de linhas do segundo fator B para que seja possível formar o produto AB. Se essa condição não for satisfeita, o produto não estará definido.

Em geral se $A = [a_{ij}]$ for uma matriz $m \times r$ e $B = [b_{ij}]$ for uma matriz $r \times n$ então o produto AB têm a forma $m \times n$ onde a entrada $(AB)_{ij}$ na linha i e na coluna j de AB é dada por

$$(AB)_{ij} = \sum_{k=1}^{r} a_{ik} b_{kj} = a_{i1} b_{1j} + a_{i2} b_{2j} + \ldots + a_{ir} b_{rj}.$$

Definição 3.6. Se A for uma matriz $m \times n$ qualquer, então a transposta de A, denotada por A^T, é definida como a matriz $n \times m$ que resulta da troca de posição das linhas com as

colunas de A; ou seja, a primeira coluna de A^T é a primeira linha de A, a segunda coluna de A^T é a segunda linha de A, e assim por diante.

Exemplo 3.3. Alguns exemplos de matrizes e suas transpostas são os seguintes. Sendo

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}, \; B = \begin{pmatrix} 1 & 2 & 54 \\ 0 & 7 & 9 \\ 9 & 4 & 5 \end{pmatrix}, \; C = \begin{pmatrix} 11 \\ 6 \end{pmatrix}, \; D = \begin{pmatrix} 5 & 1 \end{pmatrix}, \; E = \begin{pmatrix} 3 \end{pmatrix}.$$

Temos

$$A^T = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \\ a_{13} & a_{23} \end{pmatrix}, \; B^T = \begin{pmatrix} 1 & 0 & 9 \\ 2 & 7 & 4 \\ 54 & 9 & 5 \end{pmatrix}, \; C^T = \begin{pmatrix} 11 & 6 \end{pmatrix}, \; D^T = \begin{pmatrix} 5 \\ 1 \end{pmatrix}, \; E^T = \begin{pmatrix} 3 \end{pmatrix}.$$

Observemos que não só as colunas de A^T são as linhas de A, mas também as linhas de A^T são as colunas de A. Assim, a entrada na linha i e coluna j de A^T é a entrada na linha j e coluna i de A; ou seja,

$$(A^T)_{ij} = (A)_{ji}.$$

3.2 MATRIZES INVERSAS E PROPRIEDADES ALGÉBRICAS DAS MATRIZES

Admitiremos como conhecidas algumas propriedades elementares da álgebra das matrizes tais como, por exemplo, a propriedade associativa da multiplicação de matrizes, e a propriedade distributiva da multiplicação em relação à adição, ou seja, para matrizes $A_{m\times n}$, $B_{n\times r}$, $C_{n\times r}$, $D_{r\times s}$, temos

$$A(BD) = (AB)D,$$
$$A(B + C) = AB + AC,$$
$$(B + C)D = BC + BD.$$

Uma matriz A com a forma $m \times n$ onde $n = m$ é denominada *matriz quadrada* de ordem n.

Definição 3.7 (Matriz Identidade)**.** Uma matriz quadrada com entradas iguais a 1 na diagonal principal e demais entradas nulas é denominada **matriz identidade**.

Exemplo 3.4. Alguns exemplos de matrizes identidade

$$\begin{pmatrix}1\end{pmatrix}, \quad \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}, \quad \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}.$$

Em geral uma matriz identidade é denotada por I. Se for importante enfatizar seu tamanho escrevemos I_n para a matriz identidade de tamanho $n \times n$. A matriz identidade, na aritmética matricial, exerce o papel de "elemento neutro" na multiplicação de matrizes. Isto é traduzido pela seguinte propriedade, que admitiremos sem demonstração.

Seja $A_{m\times n}$ então

$$I_m A = A = A I_n.$$

Definição 3.8 (Matriz Inversa)**.** Se A for uma matriz quadrada e se pudermos encontrar uma matriz B de mesmo tamanho tal que $AB = BA = I$, então diremos que A é **inversível** (ou **não singular**) e que B é uma **inversa** de A. Se não puder ser encontrada uma tal matriz B, diremos que A é **não inversível** (ou **singular**).

A relação $AB = BA = I$ permanece inalterada pela troca de A por B, de modo que se A for inversível e B uma inversa, então também vale que B é inversível e que A é uma inversa de B. Assim, se

$$AB = BA = I.$$

dizemos que A e B são inversas uma da outra.

Teorema 3.1. *Se* B *e* C *são ambas inversas da matriz* A*, então* $B = C$*.*

Demonstração. Como B é inversa de A temos $BA = I$. Multiplicando ambos os lados à direita por C dá $(BA)C = IC = C$. Mas também vale que $(BA)C = B(AC) = BI = B$, de modo que $B = C$ ■

Como uma consequência desse importante resultado, podemos agora falar da inversa de uma matriz inversível. Se A for inversível, então sua inversa será denotada pelo símbolo A^{-1}. Assim,

$$AA^{-1} = A^{-1}A = I$$

Definição 3.9. Sendo $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ a quantidade $a_{11}a_{22} - a_{21}a_{12}$ é denominada **determinante** da matriz A, denotada por $\det(A) = a_{11}a_{22} - a_{21}a_{12}$

Admitiremos também, sem demonstração, a seguinte proposição, fácil de ser demonstrada no caso $n = 2$.

Proposição 3.1. *Se A e B são matrizes quadradas de ordem n então*

$$\det(AB) = \det(A) \cdot \det(B)$$

Uma demonstração é encontrada em (ANTON; RORRES, 2012, p. 109).

Teorema 3.2. *A matriz*

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

é inversível se, e somente se, $\det(A) \neq 0$*, caso em que a inversa de A é dada por*[1]

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

Demonstração.

($\Rightarrow$) Se existe a matriz inversa A^{-1} então $AA^{-1} = I_2$ e $\det(AA^{-1}) = \det(I_2) = 1$, por outro lado temos, usando a Proposição 3.1,
$1 = \det(I_2)\det(AA^{-1}) = \det(A) \cdot \det(A^{-1}) \Rightarrow \det(A) \neq 0$.

($\Leftarrow$) Se $\det(A) \neq 0$ então consideremos a matriz $B = \frac{1}{\det(A)} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$. Temos

$$\begin{aligned} A \cdot B &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} \frac{a_{22}}{\det(A)} & \frac{-a_{12}}{\det(A)} \\ \frac{-a_{21}}{\det(A)} & \frac{a_{11}}{\det(A)} \end{pmatrix} \\ &= \begin{pmatrix} \frac{a_{11}a_{22} - a_{21}a_{12}}{\det(A)} & \frac{-a_{11}a_{12} + a_{11}a_{12}}{\det(A)} \\ \frac{a_{21}a_{22} - a_{21}a_{22}}{\det(A)} & \frac{-a_{21}a_{12} + a_{11}a_{22}}{\det(A)} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2. \end{aligned}$$

Analogamente podemos mostrar que $B \cdot A = I_2$, portanto A é inversível e $B = A^{-1}$. ■

[1] Sendo $A = (a_{ij})$ uma matriz e λ um número real, define-se a matriz $\lambda A = (c_{ij})$, em que $c_{ij} = \lambda a_{ij}$ para cada i e cada j.

3.3 ARITMÉTICA MODULAR

Esta seção apresenta requisitos básicos de teoria dos números, especificamente sobre a *aritmética de resíduos módulo* m, necessários para uma compreensão matemática da criptografia RSA. Tal conceito também é requisito parcial à compreensão das cifras de Hill.

De acordo com Hefez (2016, p. 166), o estudo sobre *aritmética modular*, ou simplesmente, *aritmética dos restos*, foi introduzido por Gauss (1777–1855) em seu livro *Disquisitiones Arithmeticae*, de 1801. Tal ramo da matemática trata de sistematizar operações para obter resultados sobre restos de divisões euclidianas de inteiros.

Os conceitos de aritmética dos inteiros tratados neste capítulo foram coletados e uniformizados a partir de três referências, (HEFEZ, 2016), (MILIES, 2020), e (ROSEN, 1993).

Assumiremos conhecido o conjunto $\mathbb{Z}$ dos números inteiros com suas duas operações elementares, a adição e a multiplicação, e uma relação de ordem $\leq$. Assumiremos que o conjunto $\mathbb{N}$, dos números naturais é um subconjunto de $\mathbb{Z}$, sendo $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}$.

Dados a e $m \in \mathbb{Z}$, $m \neq 0$, é sempre possível efetuar a divisão de a por m e obter um resto r. Tal conceito é apresentado a seguir e a sua compreensão é fundamental para o desenvolvimento da aritmética modular.

Seja $A \subset \mathbb{Z}$, $A \neq \emptyset$. Dizemos que um número inteiro a é um *menor elemento* de A se as seguintes propriedades são verdadeiras:

(i) $a \in A$

(ii) para cada $n \in A$, $a \leq n$

Definição 3.10. Dizemos que um conjunto A de inteiros é *limitado inferiormente* se existe um inteiro k tal que $k \leq a$, para todo elemento $a \in A$.

Propriedade da Boa Ordem. Todo subconjunto não vazio e limitado inferiormente de $\mathbb{Z}$, possui um menor elemento.

Definição 3.11. Dados dois números inteiros a e b (com $b \neq 0$), dizemos que b **divide** a (ou que b é um **divisor** ou um **fator** de a) se existe um inteiro c tal que $a = bc$. Neste caso, também dizemos que a é um **múltiplo** de b. O inteiro c nestas condições chama-se o **quociente** de a por b.

Usaremos a notação $b \mid a$ para indicar que b divide a. Para negar esta afirmação escrevemos $b \nmid a$. Quando $b \mid a$, o quociente de a por b será representado alternativamente

na forma

$$c = a/b \quad \text{ou} \quad c = \frac{a}{b}.$$

Teorema 3.3 (Algoritmo da Divisão Euclidiana)**.** *Sejam* a *e* b *números inteiros, com* $b > 0$*. Então existem dois únicos números inteiros,* q *e* r*, tais que*

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

Demonstração. Consideremos o conjunto $\mathcal{S}$ de todos os inteiros da forma $a - bk$ onde k é um inteiro, ou seja, $\mathcal{S} = \{a - bk \mid k \in \mathbb{Z}\}$.

Seja $\mathcal{T}$ o conjunto de todos os inteiros não negativos de $\mathcal{S}$. $\mathcal{T}$ é não vazio, pois $a - bk$ é positivo sempre que $k < a/b$. Pela Propriedade da Boa Ordem, $\mathcal{T}$ possui uma elemento mínimo $r = a - bq$ (estes serão o valores para q e r especificados do teorema).

Sabemos que $r \geq 0$ por construção, e é fácil ver que $r < b$. Caso $r \geq b$ temos $r > r - b = a - bq - b = a - b(q + 1) \geq 0$ que contradiz a escolha de $r = a - bq$ como sendo o menor inteiro da forma $a - bk$. Portanto $0 \leq r < b$.

Para mostrarmos que esses valores para q e r são únicos, suponhamos que temos duas equações (i) $a = bq_1 + r_1$ e (ii) $a = bq_2 + r_2$, com $0 \leq r_1 < b$ e $0 \leq r_2 < b$. Subtraindo (ii) de (i) temos

$$0 = b(q_1 - q_2) + (r_1 - r_2) \Rightarrow r_2 - r_1 = b(q_1 - q_2).$$

Isso nos diz que $b \mid (r_2 - r_1)$. Como $0 \leq r_1 < b$ e $0 \leq r_2 < b$, temos $-b < r_2 - r_1 < b$. Portanto b pode dividir $r_2 - r_1$ somente quando $r_2 - r_1 = 0$, ou seja, $r_2 = r_1$.

Como $bq_1 + r_1 = bq_2 + r_2$ e $r_1 = r_2$ temos também que $q_1 = q_2$. Isso mostra que o quociente q e o resto r são únicos. ■

Por serem únicos, chamaremos q de quociente e r de resto da divisão de a por m. Temos que o resto da divisão de a por m será igual a zero se, e somente se, m divide a, isto é, m é um divisor de a. Denotaremos essa relação por $m \mid a$. Caso contrário, escrevemos $m \nmid a$.

Definição 3.12 (Máximo Divisor Comum)**.** Chamamos máximo divisor comum de dois números inteiros a e b, e denotamos por $\mathrm{mdc}(a, b)$, o maior dos seus divisores comuns. Caso $a = b = 0$ definimos $\mathrm{mdc}(a, b) = 0$.

Dados dois inteiros a e b. Dizemos que a e b são *relativamente primos* (*coprimos*) se, e somente se, $\mathrm{mdc}(a, b) = 1$.

Proposição 3.2. *Sejam* a *e* b *inteiros. Se* $b \mid a$ *e* $a \neq 0$ *então* $|b| \leq |a|$ *ou, equivalentemente* $-|a| \leq b \leq |a|$.

Demonstração. Se $b \mid a$ então existe um inteiro c tal que $a = bc$. Tomando módulos em ambos os membros temos que $|bc| = |b| \cdot |c| = |a|$. Como c é um inteiro não nulo, temos que

$$1 \leq |c|.$$

Multiplicando ambos os membros desta desigualdade por $|b|$ temos

$$|b| \leq |b| \cdot |c| = |a|$$

e equivalentemente $-|a| \leq b \leq |a|$. ■

Teorema 3.4. *Dados dois inteiros* a *e* b*, com* $a \neq 0$ *ou* $b \neq 0$*, existem inteiros* r *e* s *tais que*

$$\mathrm{mdc}(a, b) = ra + sb.$$

Demonstração. Consideremos o conjunto

$$\mathcal{S} = \{xa + yb \mid x, y \in \mathbb{Z},\ xa + yb > 0\}.$$

Claramente, $\mathcal{S}$ é não vazio pois caso tenhamos $b \neq 0$ temos

$$(i)\ b > 0 \Rightarrow 0 \cdot a + 1 \cdot b \in \mathcal{S} \quad \text{ou} \quad (ii)\ b < 0 \Rightarrow 0 \cdot a + (-1) \cdot b \in \mathcal{S}.$$

Analogamente, a ou $-a$ estará em $\mathcal{S}$ se $a \neq 0$.

Então, se para algum par (x, y) de inteiros tivermos $xa + yb < 0$ basta tomarmos o par $(-x, -y)$ e teremos $-xa - yb = -(xa + yb) > 0$.

Pelo Principio da Boa Ordem, $\mathcal{S}$ tem um elemento mínimo, que denotaremos por d. Como $d \in \mathcal{S}$, ele é da forma $d = ra + sb$, com $r, s \in \mathbb{Z}$.

Vamos provar que $d = \mathrm{mdc}(a, b)$.

Começaremos mostrando que d divide a. De fato, como $d > 0$, pelo Algoritmo da Divisão Euclidiana, existem inteiros q_1 e r_1 tais que $a = dq_1 + r_1$, com $0 \leq r_1 < d$. Então temos:

$$r_1 = a - dq_1 = a - (ra + sb)q_1 = (1 - r)a + sq_1 b,$$

donde $r_1 \in \mathcal{S}$. Como $r_1 < d$, que é o mínimo de $\mathcal{S}$, se $r_1 \neq 0$ teríamos uma contradição.

Logo $r_1 = 0$ e $d \mid a$. De forma análoga temos também que $d \mid b$.

Finalmente, suponhamos que $d' > 0$ é um outro divisor comum de a e b. Então existem inteiros m e n tais que $a = md'$ e $b = nd'$. Logo,

$$d = ra + sb = rmd' + snd' = (rm + sn)d',$$

que mostra que $d' \mid d$ e implica que $d' \leq d$. Portanto d é o maior dos divisores comuns de a e b. ■

Proposição 3.3. *Dois números inteiros positivos* a *e* b *são relativamente primos se, e somente se, existem números inteiros* r *e* s *tais que* $ra + sb = 1$.

Demonstração. Suponhamos que a e b são primos entre si. Logo, $\mathrm{mdc}(a, b) = 1$. Pelo Teorema 3.4, temos que existem números inteiros r e s tais que $ra + sb = \mathrm{mdc}(a, b) = 1$, segue-se a primeira parte da proposição.

Reciprocamente, suponhamos que existam números inteiros r e s tais que $ra+sb = 1$. Se $d = \mathrm{mdc}(a, b)$, temos que $d \mid (ra + sb)$, ou seja $d \mid 1$, e, portanto, $d = 1$. ■

3.4 CONGRUÊNCIAS

Definição 3.13. Dados $a, b, m \in \mathbb{Z}$ com $m > 1$, dizemos que a e b são congruentes módulo m se obtivermos o mesmo resto ao dividirmos a e b por m. Denotaremos tal relação da seguinte forma:

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

Exemplo 3.5. Dados os números 5 e 7. Ao dividirmos por 2, obtemos resto 1 em ambos os casos. Porém ao dividirmos por 3, encontramos como resto os números 2 e 1, respectivamente. Dessa forma, podemos escrever:

$$5 \equiv 7 \pmod{2}, \quad 5 \not\equiv 7 \pmod{3}.$$

Proposição 3.4. *Sejam* $a, b, m \in \mathbb{Z}$ *com* $m > 1$*, temos* $a \equiv b \pmod{m}$ *se, e somente se,* $m \mid (b - a)$.

Demonstração. Pelo Algoritmo de divisão de Euclides, existem quocientes $q_1, q_2 \in \mathbb{Z}$ e restos $r_1, r_2 \in \mathbb{Z}$ tais que $0 \leq r_1, r_2 < m$, $a = mq_1 + r_1$ e $b = mq_2 + r_2$. Assim,

$$b - a = mq_2 + r_2 - mq_1 - r_1 = m(q_2 - q_1) + (r_2 - r_1).$$

Uma vez que $a \equiv b \pmod{m}$, temos que o resto da divisão de a e b por m é o mesmo, isto é,

$$r_1 = r_2 \Rightarrow r_2 - r_1 = 0,$$

o que significa que $b - a = m(q_2 - q_1)$ e portanto $m \mid (b - a)$.

Reciprocamente, suponhamos que $m \mid (b - a)$.

Como $m \mid m$, segue que $m \mid m(q_2 - q_1)$ e consequentemente

$$m \mid (b - a) - m(q_2 - q_1) \Rightarrow m \mid (r_2 - r_1).$$

Agora, como $0 \leq r_1, r_2 < m$, temos

$$-(m - 1) \leq r_2 - r_1 \leq m - 1.$$

No intervalo acima, somente 0 é divisível por m, e portanto $r_2 = r_1$, logo:

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

■

Proposição 3.5. *Seja $m \in \mathbb{N}$ com $m > 1$. Para todos $a, b, c \in \mathbb{Z}$, temos que*

(i) $a \equiv a \pmod{m}$ *(Reflexividade),*

(ii) Se $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$ *(Simetria),*

(iii) Se $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$, *então* $a \equiv c \pmod{m}$ *(Transitividade).*

Demonstração. Pela Proposição 3.4, temos que $a \equiv b \pmod{m} \Leftrightarrow m \mid (b - a)$.

(i) $m \mid 0 \Rightarrow m \mid (a - a) \Rightarrow a \equiv a \pmod{m}$.

(ii) Se $a \equiv b \pmod{m}$, temos que $m \mid (b - a)$ e $m \mid -(b - a)$, ou seja,

$$m \mid (-b + a) \Rightarrow m \mid (a - b) \Rightarrow b \equiv a \pmod{m}$$

(iii) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ então $m \mid (b - a)$ e $m \mid (c - b)$.

Daí,

$$b - a = mq \tag{3.1}$$

$$c - b = mq' \tag{3.2}$$

Da equação (3.1), é possível concluir que $b = a + mq$. Substituindo em (3.2), temos:

$$c - (a + mq) = mq' \Rightarrow c - a = mq' + mq \Rightarrow c - a = m(q' + q)$$

$$\Rightarrow c - a = mq", \text{ com } q" = (q' + q).$$

Logo, $m \mid (c - a)$, ou seja, $a \equiv c \pmod{m}$. ■

Proposição 3.6. *Sejam* $a, b, c, d, m \in \mathbb{Z}$, *com* $m > 1$.

(i) Se $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $a + c \equiv b + d \pmod{m}$.

(ii) Se $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $a - c \equiv b - d \pmod{m}$.

(iii) Se $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $ac \equiv bd \pmod{m}$.

Demonstração. Suponhamos que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Então $m \mid (b - a)$ e $m \mid (d - c)$, ou seja, $b - a = mq$ e $d - c = mq'$.

(i) Temos que $(b-a)+(d-c) = mq+mq'$, ou seja, $(b+d)-(a+c) = m(q+q') = mq''$. Daí, $m \mid (b + d) - (a + c)$, isto é, $(a + c) \equiv (b + d) \pmod{m}$.

(ii) Temos que $(a - c) - (b - d) = (a - b) - (c - d) = pm - qm = (p - q)m$. Daí $m \mid (a - c) - (b - d)$, ou seja $a - c \equiv b - d \pmod{m}$

(iii) Observe que $bd - ac = bd + ad - ad - ac = d(b - a) + a(d - c)$. Por hipótese, $m \mid (b - a)$ e $m \mid (d - c)$, isto é, $m \mid d(b - a) + a(d - c)$, ou seja, $m \mid bd - ac$.

Portanto, $ac \equiv bd \pmod{m}$. ■

Proposição 3.7. *Sejam* $a, b, c \in \mathbb{Z}$, *sendo* a *e* b *não simultaneamente nulos e* $c > 0$. *Seja* $d = \text{mdc}(a, b)$. *Então*

a) $\text{mdc}(ac, bc) = c \cdot \text{mdc}(a, b)$.

b) Se $c \mid a$ *e* $c \mid b$ *então* $c \mid d$ *e* $\text{mdc}(\frac{a}{c}, \frac{b}{c}) = \frac{d}{c}$.

c) Sendo $d = \text{mdc}(a, b)$, *temos* $\frac{a}{d}$ *e* $\frac{b}{d}$ *primos entre si.*

Demonstração. a) Seja $d = \text{mdc}(a, b)$. Então $d \mid a$ e $d \mid b$, logo $dc \mid ac$ e $dc \mid bc$.

Pelo Teorema 3.4, existem inteiros r, s tais que $ra + sb = d$. Logo $r(ac) + s(bc) = dc$. Se x é um inteiro positivo tal que $x \mid ac$ e $x \mid bc$ então $x \mid (r(ac) + s(bc))$, ou seja, $x \mid dc$, logo $x \leq dc$.

Portanto, $dc = \text{mdc}(ac, bc)$.

b) Usando o resultado do item anterior, temos $c \cdot \mathrm{mdc}(\frac{a}{c}, \frac{b}{c}) = \mathrm{mdc}(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}) = \mathrm{mdc}(a, b) = d$, logo $\mathrm{mdc}(\frac{a}{c}, \frac{b}{c}) = \frac{d}{c}$.

c) Tomando $c = d$ no resultado do item 2, temos $\mathrm{mdc}(\frac{a}{d}, \frac{b}{d}) = \frac{d}{d} = 1$, portanto $\frac{a}{\mathrm{mdc}(a,b)}$ e $\frac{b}{\mathrm{mdc}(a,b)}$ são inteiros coprimos. ■

Proposição 3.8. *Sejam* a, b, c *inteiros, com* a *e* b *primos entre si. Então*

$$a \mid bc \iff a \mid c.$$

Demonstração. Obviamente se $a \mid c$ então $a \mid bc$.

Suponhamos que $a \mid bc$. Então $bc = ax$ para algum inteiro x.

Sendo a e b primos entre si, pelo Corolário 3.3, existem inteiros r e s tais que $ra + sb = 1$. Daí $rac + sbc = c$.

Como $bc = ax$, temos então $rac + sax = c$, logo $c = a(rc + rx)$ e portanto $a \mid c$. ■

Proposição 3.9. *Sejam* $a, b, c, m \in \mathbb{Z}$*, com* $c \neq 0$ *e* $m > 1$*. Temos que*

$$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \left(\mathrm{mod}\ \frac{m}{\mathrm{mdc}(c,m)}\right).$$

Demonstração. Podemos supor, sem perda de generalidade, que $bc \geq ac$. Como $\frac{m}{\mathrm{mdc}(c,m)}$ e $\frac{c}{\mathrm{mdc}(c,m)}$ são coprimos, temos que

$$\begin{aligned}
ac \equiv bc \pmod{m} &\iff m \mid (b-a)c \\
&\iff (b-a)c = mq \quad (q \in \mathbb{Z}) \\
&\iff (b-a) \cdot \frac{c}{\mathrm{mdc}(c,m)} = \frac{m}{\mathrm{mdc}(c,m)} q \quad (q \in \mathbb{Z}) \\
&\iff \frac{m}{\mathrm{mdc}(c,m)} \text{ divide } (b-a) \cdot \frac{c}{\mathrm{mdc}(c,m)} \\
&\iff \frac{m}{\mathrm{mdc}(c,m)} \mid (b-a) \\
&\iff a \equiv b \left(\mathrm{mod}\ \frac{m}{\mathrm{mdc}(c,m)}\right).
\end{aligned}$$

■

Corolário 3.1. *Sejam* $a, b, c, m \in \mathbb{N}$*, com* $m > 1$ *e* $\mathrm{mdc}(c, m) = 1$*. Temos que*

$$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{m}.$$

Dado um inteiro $m > 1$, qualquer inteiro a é equivalente (congruente), módulo m, a

exatamente um dos inteiros $0, 1, 2, \ldots, m-1$, pois o resto da divisão de a por m está no conjunto $\{0, 1, \ldots, m-1\}$.

Esse inteiro é denominado resíduo de a módulo m e escrevemos

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

para denotar um *sistema completo de resíduos módulo* m.

Também dizemos que um conjunto $\{a_1, \ldots, a_m\}$ é um sistema completo de resíduos módulo m quando, a menos de congruência módulo m, esse conjunto coincide com o conjunto $\{0, 1, \ldots, m-1\}$.

Pela Proposição 3.6, podemos definir operações de adição e multiplicação em $\mathbb{Z}_m$, de modo que $a + b = c$ e $ab = d$ se e somente se $a + b \equiv c \pmod{m}$ e $ab \equiv d \pmod{m}$.

Definição 3.14. Um *sistema reduzido de resíduos* módulo m é um conjunto de números naturais $r_1, \ldots, r_s$, tais que

(i) $\mathrm{mdc}(r_i, m) = 1$, para cada $i \in \{1, \ldots, s\}$.

(ii) $r_i \not\equiv r_j \pmod{m}$, se $i \neq j$

(iii) Para cada $n \in \mathbb{N}$ tal que $\mathrm{mdc}(m, n) = 1$, existe i tal que $n \equiv r_i \pmod{m}$.

Pode-se obter um sistema reduzido de resíduos $r_1, \ldots, r_s$, módulo m, a partir de um sistema completo qualquer de resíduos $a_1, \ldots, a_m$, módulo m, eliminando os elementos a_i que não são primos com m.

Proposição 3.10. *Dados um inteiro* a *e um módulo* m *quaisquer, seja*

$$R = \textit{resto da divisão de } |a| \textit{ por } m$$

Então o resíduo r *de* a *módulo* m*,* $0 \leq R \leq m-1$*, é dado por*

$$r = \begin{cases} R, & \textit{se } a \geq 0 \\ m - R, & \textit{se } a < 0 \quad \textit{e} \quad R \neq 0 \\ 0, & \textit{se } a < 0 \quad \textit{e} \quad R = 0 \end{cases}$$

Definição 3.15. Dado um número a em $\mathbb{Z}_m$, dizemos que um número a^{-1} em $\mathbb{Z}_m$ é um **recíproco**, ou **inverso multiplicativo**, de a módulo m se $aa^{-1} = a^{-1}a \equiv 1 \pmod{m}$.

Proposição 3.11. *Sejam* $a, b \in \mathbb{Z}$ *e* $m, n, m_1, \ldots, m_r$ *inteiros maiores que 1. Seja* $[m_1, \ldots, m_r]$ *o mínimo múltiplo comum de* $m_1, \ldots, m_r$*. Temos que*

(i) *se* $a \equiv b \pmod{m}$ *e* $n \mid m$*, então* $a \equiv b \pmod{n}$;

(ii) *se* $a \equiv b \pmod{m_i}$*, para cada* $i \in \{1, \ldots, r\} \Leftrightarrow a \equiv b \pmod{\{)[m_1, \ldots, m_r]\}}$.

Demonstração. (i) Se $a \equiv b \pmod{m}$, então $m \mid (b - a)$. Como $n \mid m$, segue-se que $n \mid (b - a)$. Logo, $a \equiv b \pmod{n}$.

(ii) Se $a \equiv b \pmod{m_i}$, $i = 1, \ldots r$, então $m_i \mid (b - a)$ para cada i. Sendo $b - a$ um múltiplo de cada m_i, segue-se que $[m_1, \ldots, m_r] \mid (b - a)$, o que prova que $a \equiv b \pmod{[m_1, \ldots, m_r]}$.

A recíproca decorre do item (i). ■

Teorema 3.5 (Teorema Chinês dos Restos)**.** *Sejam* $m_1, m_2, ..., m_r$ *inteiros positivos dois a dois relativamente primos. Então o sistema de congruências*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases} \tag{3.3}$$

tem uma solução única módulo $M = m_1 m_2 \ldots m_r$*. Os inteiros soluções de (3.3) tem a forma*

$$x = M_1 y_1 a_1 + \cdots + M_r y_r a_r + tM,$$

em que $t \in \mathbb{Z}$*,* $M_i = M/m_i$ *e* y_i *é a solução de* $M_i y \equiv 1 \pmod{m_i}, \quad i = 1, \ldots, r$.

Demonstração. Vamos inicialmente, provar que x é uma solução simultânea do sistema (3.3). De fato, como $m_i \mid M_j$, se $i \neq j$ e $M_i y_i \equiv 1 \pmod{m_i}$, temos que

$$x = M_1 y_1 a_1 + \cdots + M_r y_r a_r \equiv M_i y_i a_i \equiv a_i \pmod{m_i}.$$

Por outro lado, se x' é outra solução do sistema (3.3), então

$$x \equiv x' \pmod{m_i} \text{ para cada } i \in \{1, \ldots r\}.$$

Como $\mathrm{mdc}(m_i, m_j) = 1$, para $i \neq j$, segue-se que $[m_1, \ldots, m_r] = m_1 \cdots m_r = M$ e consequentemente pela Proposição 3.11 temos que $x \equiv x' \pmod{M}$. ■

Definição 3.16 (Função fi de Euler)**.** Designamos por $\varphi(m)$ o número de elementos de um *sistema reduzido de resíduos módulo* $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Pondo $\varphi(1) = 1$, isso define uma função

$$\varphi : \mathbb{N} \to \mathbb{N}$$

chamada *função fi de Euler*.

Proposição 3.12. *Seja p um número primo, então $\varphi(p) = p - 1$. Reciprocamente, se p é um inteiro positivo com $\varphi(p) = p - 1$, então p é um número primo.*

Demonstração. Se p é um número primo então qualquer inteiro positivo menor que p é relativamente primo com p, como estes são $p - 1$ elementos temos $\varphi(p) = p - 1$.

Reciprocamente, se p é um número não primo, então $p = 1$ ou p é composto. Se $p = 1$, então $\varphi(p) \neq p - 1$ pois temos que $\varphi(1) \doteq 1$. Se p é composto, então p tem um divisor d com $1 < d < p$ e p e d não são relativamente primos. Como sabemos que pelo menos um dos $p - 1$ inteiros $1, 2, \ldots, p - 1$, justamente d, não é relativamente primo com p, temos $\varphi(p) \leq p - 2$. Portanto, se $\varphi(p) = p - 1$, concluímos que p é primo. ■

Proposição 3.13. *Sejam p um número primo e a um número inteiro positivo. Então $\varphi(p^a) = p^a - p^{a-1}$.*

Demonstração. Os inteiros positivos menores ou iguais a p^a que não são relativamente primos com p são aqueles inteiros que não excedem p^a e que são divisíveis por p. Estes são os inteiros kp, onde $1 \leq k \leq p^{a-1}$. Como existem exatamente p^{a-1} inteiros que satisfazem isto, então são em número de $p^a - p^{a-1}$ os inteiros menores que p^a que são relativamente primos com p^a. Portanto, $\varphi(p^a) = p^a - p^{a-1}$. ■

Proposição 3.14. *Sejam m, n números naturais não nulos tais que $\mathrm{mdc}(m, n) = 1$. Então*

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Por esta propriedade, dizemos que a função φ é multiplicativa*.*

Demonstração. Consideremos os inteiros positivos de 1 a mn dispostos como na seguinte

tabela.

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\vdots & \vdots & \vdots & & \vdots \\
r & m+r & 2m+r & \cdots & (n-1)m+r \\
\vdots & \vdots & \vdots & & \vdots \\
m & 2m & 3m & \cdots & mn
\end{array}$$

Agora, suponhamos que r seja um número inteiro positivo menor ou igual a m, não primo com m, isto é com $\mathrm{mdc}(m, r) = d > 1$.

Teremos então que nenhum número na r-ésima linha é relativamente primo com mn, pois qualquer elemento desta linha tem a forma $km + r$, onde k é um inteiro com $1 \leq k \leq n-1$ e $d \mid (km + r)$, pois $d \mid m$ e $d \mid r$.

Consequentemente, para encontrar os números inteiros na tabela que são relativamente primos com mn, precisamos olhar para a r-ésima linha apenas se $\mathrm{mdc}(m, r) = 1$.

Se $\mathrm{mdc}(m, r) = 1$ e $1 \leq r \leq m$, devemos determinar quantos inteiros nesta linha são relativamente primos com mn.

Os elementos nesta linha são,

$$r,\ m+r,\ 2m+r, \ldots,\ (n-1)m+r.$$

Como $\mathrm{mdc}(r, m) = 1$, cada um desses inteiros é relativamente primo com m.

Pelo Corolário 3.1 os n inteiros na linha formam um sistema completo de resíduos módulo n, pois sendo $\mathrm{mdc}(m, n) = 1$, temos $km + r \equiv k + r \pmod{n}$.

Além disso, a aplicação $k \mapsto k + r$ é injetora, sendo $k + r \equiv k' + r \pmod{n}$ se e somente se $k \equiv k' \pmod{n}$. Assim os inteiros $r,\ 1 + r, \ldots, m - 1 + r$ são um sistema completo de resíduos módulo n.

Portanto, exatamente $\varphi(n)$ desses inteiros são relativamente primos com n. Esses $\varphi(n)$ inteiros também são relativamente primos com m, sendo eles os inteiros da linha que são relativamente primos com mn. E como existem $\varphi(m)$ linhas de elementos primos com m, cada uma contendo $\varphi(n)$ inteiros relativamente primos a mn, podemos concluir que

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

■

Proposição 3.15. *Seja* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *a fatoração em potências de números primos do inteiro positivo* n*. Então*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Demonstração. Seja n um inteiro positivo, com $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Como a função φ é multiplicativa, e pela Proposição 3.14 temos

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})$$

Agora usando a Proposição 3.13 temos também que

$$\varphi(p_j^{\alpha_j}) = p_j^{\alpha_j} - p_{j-1}^{\alpha_{j-1}} = p_j^{\alpha_j}\left(1 - \frac{1}{p_j}\right) \qquad j = 1, 2, \ldots, k.$$

Assim

$$\begin{aligned}\varphi(n) &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)\\ &= p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).\end{aligned}$$

■

Proposição 3.16. *Seja* $r_1, \ldots, r_{\varphi(m)}$ *um sistema reduzido de resíduos módulo* m *e seja* $a \in \mathbb{N}$ *tal que* $\mathrm{mdc}(a, m) = 1$*. Então,* $ar_1, \ldots, ar_{\varphi(m)}$ *é um sistema reduzido de resíduos módulo* m*.*

Demonstração. Sendo p, q, r inteiros, se $\mathrm{mdc}(p, q) = 1$ e $\mathrm{mdc}(p, r) = 1$ então $\mathrm{mdc}(p, qr) = 1$. Pois neste caso temos $xp + yq = 1$ e $zp + wr = 1$ para certos inteiros x, y, z, w. Multiplicando membro a membro essas igualdades, obtemos $xzp^2 + xwpr + yzqp + ywqr = 1$ e então $(pxz + xwr + yzq)p + (yw)qr = 1$ e portanto $\mathrm{mdc}(p, qr) = 1$.

Assim, sendo $\mathrm{mdc}(a, m) = 1$ e $\mathrm{mdc}(r_i, m) = 1$ vem $\mathrm{mdc}(ar_i, m) = 1$ para $i = 1, \ldots, \varphi(m)$.

Além disso $ar_i \equiv ar_j \pmod{m}$ se, e somente se, $r_i \equiv r_j \pmod{m}$.

Portanto, $ar_1, \ldots, ar_{\varphi(m)}$ são $\varphi(m)$ resíduos reduzidos módulo m, distintos entre si, sendo então todos os $\varphi(m)$ resíduos reduzidos módulo m. ■

Teorema 3.6 (Teorema de Euler)**.** *Sejam* $m, a \in \mathbb{Z}$ *com* $m > 1$ *e* $\mathrm{mdc}(a, m) = 1$*. Então,*

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

Demonstração. Seja $r_1, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Pela Proposição 3.16, $ar_1, \ldots, ar_{\varphi(m)}$ formam um sistema reduzido de resíduos módulo m.

Portanto,

$$a^{\varphi(m)} r_1 \cdot r_2 \cdots r_{\varphi(m)} = ar_1 \cdot ar_2 \cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(m)} \pmod{m}.$$

Como $\mathrm{mdc}(r_1 \cdot r_2 \cdots r_{\varphi(m)}, m) = 1$, segue-se pelo Corolário 3.1 que

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

■

Corolário 3.2 (Pequeno Teorema de Fermat)**.** *Sejam* $a, p \in \mathbb{N}$*, onde* p *é um número primo e* $\mathrm{mdc}(a, p) = 1$*. Temos que*

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

Demonstração. Basta notarmos que, sendo p primo e pela Proposição 3.12 temos que,

$$\varphi(p) = p - 1.$$

■

4 CRIPTOGRAFIA

A palavra *criptografia* deriva do Grego $\kappa\rho\pi\tau\acute{o}\sigma =$ kryptós “escondido” e $\gamma\rho\acute{\alpha}\varphi\omega =$ gráfo “escrever”.

O estudo da codificação e decodificação de mensagens secretas é denominado **criptografia**. Embora os códigos secretos remontem aos primórdios da comunicação escrita, tem havido um aumento recente de interesse na assunto devido a necessidade de manter a privacidade da informação transmitida ao longo de linhas públicas de comunicação.

Na linguagem da criptografia, os códigos são denominados **cifras**, as mensagens não codificadas são **textos comuns** e as mensagens codificadas são **textos cifrados** ou **criptogramas**. O processo de converter um texto comum não cifrado é denominado **cifrar** ou **criptografar** e o processo inverso de converter um texto cifrado não comum é denominado **decifrar**.

4.1 A EVOLUÇÃO DA ESCRITA SECRETA

As referências principais para a construção desta seção e da seguinte foram os livros de Simon Singh, sobre o desenvolvimento histórico da criptografia, (SINGH, 2001b) e (SINGH, 2001a). A formulação matemática das cifras afins é encontrada em (MILIES, 2020).

Alguns primeiros relatos da *Escrita Secreta* datam de Heródoto (485 a.C.–425 a.C.), o "pai da história". A comunicação secreta, quando é obtida através da ocultação da mensagem é conhecida como *estenografia*, nome derivado das palavras gregas *steganos*, que significa coberto, e *graphien*, que significa escrever. Em paralelo com o desenvolvimento da estenografia, houve a evolução da *criptografia*.

A criptografia pode ser dividida em dois ramos, conhecidos como *transposição* e *substituição*.

Uma das primeiras descrições de código por substituição aparece no *Kama-sutra*, texto escrito no século IV pelo estudioso brâmane *Vatsyayana* (séc. IV a.C.–séc. VI a.C.).

A *transposição* faz com que cada letra mantenha sua identidade, mas mude sua posição, enquanto a *substituição* faz com que as letras mudem de identidade mantendo a posição.

Exemplos das Cifras: considerando a mensagem AB, temos

$\mathrm{AB} \rightarrow \mathrm{BA}$ (*transposição*)

$\mathrm{AB} \rightarrow \mathrm{FM}$ (*substituição*)

O primeiro documento que usou uma cifra de substituição para propósitos militares aparece nas *Guerras de Gália* de *Júlio César*. César descreve como enviou uma mensagem para Cícero, que estava cercado, prestes a se render. Ele substituiu as letras do alfabeto romano por letras gregas, tornando a mensagem incompreensível para o inimigo.

Os criptógrafos geralmente pensam em termos do *alfabeto original*, usado para escrever a mensagem, e o *alfabeto cifrado*, formado pelas letras empregadas na substituição.

Quando o alfabeto original é colocado acima do alfabeto cifrado, como mostra a Tabela 4.1, fica claro que as letras do alfabeto original foram substituídas por letras deslocadas três casas à direita (ciclicamente, por isso X, Y e Z são substituídas por A, B e C) e por isso esta forma de substituição é frequentemente chamada de *cifra de deslocamento de César*, ou simplesmente *cifra de César*.

Tabela 4.1 – Alfabetos da cifra de César.

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

Fonte: Elaborado pelo autor.

Exemplo de cifragem usando a cifra de César dada pela Tabela 4.1.

mensagem comum: CIFRA DE CESAR

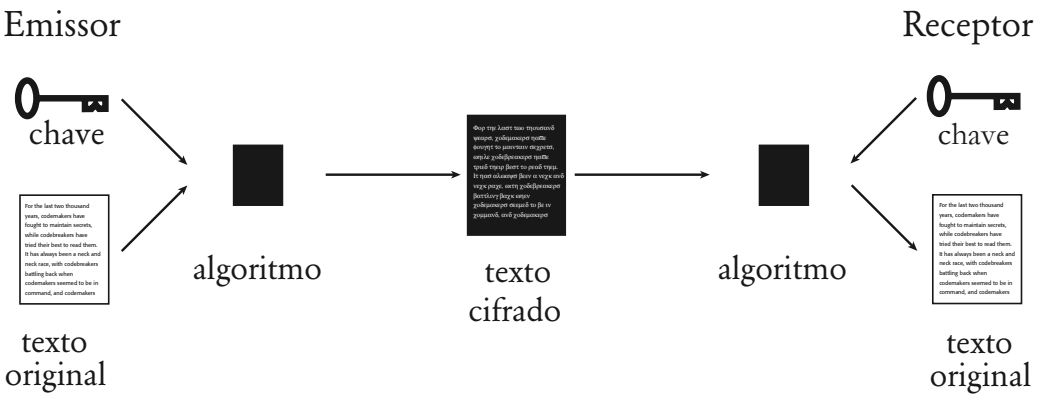
mensagem cifrada: FLIUD GH FHVDU

Cada cifra pode ser considerada em termos de um método geral de codificação conhecido como *algoritmo* e uma *chave*, que especifica os detalhes exatos de uma codificação.

Para cifrar uma mensagem, o emissor aplica ao texto a ser cifrado um algoritmo. O algoritmo é um sistema geral de cifragem, e precisa ser especificado com exatidão por meio de uma chave. A aplicação da chave e do algoritmo a uma mensagem resultará em uma mensagem cifrada, ou texto cifrado. O texto cifrado pode ser interceptado pelo inimigo enquanto é transmitido ao receptor, mas o inimigo não conseguirá (idealmente) decifrar a mensagem. O receptor, contudo, que conhece a chave e o algoritmo utilizados pelo emissor, pode converter o texto cifrado na mensagem original.

A cifra de César é muito fácil de ser interpretada matematicamente empregando a *aritmética modular*. De, fato, primeiro associamos, a cada letra, o número do lugar que ela ocupa no alfabeto, conforme a seguinte tabela.

Figura 4.1 – Esquema simplificado de codificação e decodificação de uma mensagem por chaves e algoritmos.



Fonte da ilustração: (SINGH, 2001a, p. 16).

Tabela 4.2 – Cifra de César traduzida em números.

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

Fonte: Elaborado pelo autor.

Depois, a cifra de César é aplicada usando-se a fórmula

$$C(x) = x + 3 \pmod{26},$$

sendo a variável x uma letra a ser cifrada. A soma $x + 3$ é efetuada em $\mathbb{Z}_{26}$, e a decifração de cada letra é feita empregando-se a fórmula

$$D(x) = x - 3 \pmod{26}$$

em cada letra (número) da mensagem cifrada.

Mais geralmente, se quisermos usar esta cifra, mas com período (deslocamento) n arbitrário, devem-se empregar as fórmulas:

$$C_n(x) = x + n \pmod{26},$$

$$D_n(x) = x - n \pmod{26}.$$

Assim, temos 25 possíveis cifras de César, tomando-se $1 \leq n \leq 25$.

A vantagem deste ponto de vista é que nos permite desenvolver facilmente métodos de codificação um pouco mais seguros. Por exemplo, generalizando um pouco a função afim usada na cifra de César, podemos definir a *cifra afim*, usando uma fórmula do tipo

$$f(x) = ax + b,$$

onde tanto os coeficientes quantos os valores são tomados em $\mathbb{Z}_{26}$. Nesta fórmula, b pode ser arbitrário em $\mathbb{Z}_{26}$ mas para termos uma decifração bem definida, precisamos escolher a inversível em $\mathbb{Z}_{26}$, ou seja, tal que $\mathrm{mdc}(a, 26) = 1$. Para ter uma cifragem de fato, tomamos $a \neq 1$ módulo 26.

Neste caso, a decifração é dada pela fórmula

$$x = f^{-1}(y) = a^{-1}(y - b).$$

Em termos de contagem, podemos escolher a de $\varphi(26) - 1$ modos, sendo $\varphi(26) = \varphi(2 \cdot 13) = \varphi(2) \cdot \varphi(13) = (2-1)(13-1) = 12$. São portanto 11 as possíveis escolhas de a. A saber, a deve estar no conjunto $\{3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$. Contando-se multiplicativamente as 26 possíveis escolhas de b podemos construir $11 \cdot 26 = 276$ cifras afins diferentes entre si.

Suponhamos, por exemplo, que queremos cifrar a mensagem ESTUDE usando a fórmula

$$y = 3x + 2$$

O passo inicial será transformar cada letra em seu respectivo número (conforme indicado na Tabela 4.2),

E	S	T	U	D	E
4	18	19	20	3	4

Depois, aplicamos a cada número a fórmula escolhida (lembrando que trabalhamos em $\mathbb{Z}_{26}$)

$$3 \cdot 4 + 2 = 14, \quad 3 \cdot 18 + 2 = 4, \quad 3 \cdot 19 + 2 = 7,$$

$$3 \cdot 20 + 2 = 10, \quad 3 \cdot 3 + 2 = 11, \quad 3 \cdot 4 + 2 = 14.$$

Assim, a mensagem a ser enviada será a sequência de números:

$$14 \quad 4 \quad 7 \quad 10 \quad 11 \quad 14.$$

O receptor desta mensagem, para poder decifrá-la, deverá conhecer o inverso de 3 em $\mathbb{Z}_{26}$. Para achá-lo, podemos empregar o chamado *Algoritmo de Euclides* para o cálculo do mdc, como segue, efetuamos as divisões sucessivas

$$\begin{array}{r|l} 26 & 3 \\ \hline 2 & 8 \end{array} \qquad \begin{array}{r|l} 3 & 2 \\ \hline 1 & 1 \end{array}$$

$$26 = 8 \cdot 3 + 2 \Rightarrow 2 = 26 - 8 \cdot 3,$$

$$3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 2 \cdot 1,$$

e, substituindo $2 = 26 - 8 \cdot 3$, obtemos

$$1 = 3 - (26 - 8 \cdot 3) \cdot 1 = 9 \cdot 3 - 26,$$

o que implica que $1 \equiv 9 \cdot 3 \pmod{26}$ ou, equivalentemente, que 9 é o inverso de 3 módulo 26. Logo a fórmula para decifrar a mensagem, neste caso, é

$$y = 9(x - 2),$$

que aplicada sucessivamente a cada um dos números recebidos dá

$$9 \cdot (14 - 2) = 4, \quad 9 \cdot (4 - 2) = 18, \quad 9 \cdot (7 - 2) = 19,$$

$$9 \cdot (10 - 2) = 20, \quad 9 \cdot (11 - 2) = 3, \quad 9 \cdot (14 - 2) = 4.$$

Assim recuperamos a mensagem recebida, que era, uma sequência de números,

$$4 \quad 18 \quad 19 \quad 20 \quad 3 \quad 4.$$

4.2 CIFRA DE VIGENÈRE

Reiteramos que os fatos históricos delineados nesta seção provém de (SINGH, 2001a) e (SINGH, 2001b).

Durante séculos, a cifra de substituição monoalfabética simples foi suficiente para guardar os segredos de mensagens cifradas. Mas o desenvolvimento subsequente da análise de frequências, primeiro no mundo árabe e depois na Europa, destruiu sua segurança. A trágica execução da rainha Maria, da Escócia, foi uma ilustração das fraquezas das cifras de substituição monoalfabética, e na batalha entre criptógrafos e criptoanalistas, ficou claro que os criptoanalistas tinham ganho a vantagem. Qualquer pessoa enviando uma mensagem criptografada poderia ter sua mensagem interceptada e decifrada por criptoanalistas. Aos criptógrafos foi dada a tarefa de inventar uma cifra nova e mais forte, algo que poderia enganar os criptoanalistas. Embora esta cifra não tenha historicamente surgido até o final do século XVI, suas origens podem ser rastreadas até o polímata[1] florentino do século XV, Leon Battista Alberti (1404–1472). Nascido em 1404, Alberti foi uma das principais figuras da Renascença, tendo sido pintor, compositor, poeta e filósofo, bem como o autor da primeira análise científica de perspectiva. Porém, ele é mais conhecido como arquiteto, tendo projetado a primeira Fonte de Trevi e tendo escrito *De re aedificatoria*, o primeiro livro impresso sobre arquitetura, que atuou como um catalisador para a transição do design gótico para o renascentista. Em algum momento da década de 1460, Alberti estava em visita ao Vaticano quando encontrou-se com seu amigo Leonardo Dato, o secretário pontifício, que começou a conversar com ele sobre alguns dos pontos mais delicados da criptografia. Esta conversa casual levou Alberti a escrever um ensaio sobre o assunto, delineando o que ele acreditava ser uma nova forma de cifra. Naquela época, todas as cifras de substituição exigiam um único alfabeto cifrado para criptografar cada mensagem. No entanto, Alberti propôs usar dois ou mais alfabetos cifrados e alternando entre eles durante a codificação, confundindo criptoanalistas em potencial (SINGH, 2001b).

Tabela 4.3 – (1) Alfabeto original; (2) Alfabeto cifrado 1; (3) Alfabeto cifrado 2.

(1)	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
(2)	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
(3)	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: Elaborado pelo autor.

Por exemplo, na Tabela 4.3 temos dois possíveis alfabetos cifrados, e poderíamos criptografar uma mensagem alternando entre eles. Para criptografar a mensagem **outono**, criptografaríamos a primeira letra de acordo com o Alfabeto cifrado 1, para que a letra **o** se tornasse **D**, e nós criptografariamos a segunda letra de acordo com o Alfabeto cifrado

[1] Pessoa que tem conhecimento em muitas ciências; quem conhece ou estudou muitas ciências: Leonardo da Vinci é talvez o mais famoso polímata do nosso tempo.

2, de modo que **u** se torna **C**. Para criptografar a terceira letra, retornaríamos ao Alfabeto cifrado 1, e para criptografar a quarta letra retornaríamos ao Alfabeto cifrado 2, para criptografar a quinta letra retornaríamos ao Alfabeto cifrado 1. A letra final **o**, é cifrada de acordo com o Alfabeto cifrado 2 e torna-se **J**. Portanto texto cifrado completo é **DCGJSJ**. A vantagem crucial do sistema de Alberti é que a mesma letra no texto comum não aparece necessariamente como a mesma letra no texto cifrado, neste caso, a letra inicial **o** e a letra final **o** aparecem com letras cifradas diferentes.

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. Esta tarefa coube a um grupo diferente de intelectuais que aperfeiçoaram a ideia original.

Primeiro apareceu Johannes Trithemius (1462–1536), um abade alemão, depois Giovanni Battista della Porta (1535–1615), um cientista italiano, e finalmente o diplomata francês Blaise de Vigenère (1523–1596), nascido em 1523. Vigenère tomou conhecimento dos trabalhos de Alberti, Trithemius e Porta quando, com a idade de 26 anos, ele foi enviado a Roma em uma missão de dois anos. Para começar, seu interesse em criptografia era puramente prático e estava ligado ao seu trabalho.

Então, aos trinta e nove anos, Vigenère concluiu que havia acumulado dinheiro suficiente para ser capaz de abandonar sua carreira e se concentrar em uma vida de estudos. Foi só então que ele examinou em detalhes as ideias de Alberti, Trithemius e Porta, misturando-as para formar uma nova cifra coerente e poderosa, agora conhecida como a Cifra de Vigenère. A força da cifra de Vigenère está em seu uso de não um ou dois, mas vinte e seis alfabetos criptográficos distintos para criptografar uma mensagem.

A primeira etapa da criptografia é desenhar um chamado quadrado de Vigenère, como mostrado na Tabela 4.4, um texto comum seguido por vinte e seis alfabetos cifrados, cada um deslocado por uma letra em relação ao alfabeto anterior. Consequentemente, a linha 1 representa um alfabeto cifrado com uma mudança de César de 1, que significa que pode ser usado para implementar uma cifra de deslocamento de César em que cada letra do texto simples é substituída pela letra um lugar adiante no alfabeto. Da mesma forma, a linha 2 representa um alfabeto cifrado com deslocamento de César de 2 e assim por diante. A linha no topo do quadrado, em minúsculas, representa as letras do texto comum. Você pode codificar cada letra do texto simples de acordo com qualquer um dos vinte e seis alfabetos cifrados. Por exemplo, se o alfabeto cifrado número 2 for usado, a letra **a** será cifrada como **C**, mas se o alfabeto cifrado número 12 for usado, então **a** será cifrada como **M**. Se o remetente fosse usar apenas um dos alfabetos cifrados para criptografar uma

Tabela 4.4 – Quadrado de Vigenère

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

Fonte: Elaborado pelo autor.

mensagem inteira, isso seria efetivamente um simples Cifra de César, que seria uma forma muito fraca de criptografia, facilmente decifrada por um interceptador inimigo.

No entanto, na cifra de Vigenère, linhas diferentes do quadrado de Vigenère (um alfabeto cifrado diferente) são usadas para criptografar letras em posições diferentes da mensagem.

Em outras palavras, o remetente pode criptografar a primeira letra de acordo com a linha 5, a segunda de acordo com a linha 14, a terceira de acordo com a linha 21 e

assim por diante. Para decifrar a mensagem, o receptor pretendido precisa saber qual linha do quadrado de Vigenère foi usada para cifrar cada letra, então deve haver um sistema acordado de alternação entre as linhas. Isso é feito usando uma palavra-chave. Para ilustrar como uma palavra-chave é usada com o quadrado de Vigenère para criptografar uma mensagem de amostra, vamos codificar **criptografia revelada**, usando a palavra-chave SAMAEL como mensagem e repetida indefinidamente novamente, quantas vezes for necessário, de modo que cada letra da mensagem seja associada a uma letra da palavra-chave. Usando a palavra-chave o texto cifrado é então gerado da seguinte forma.

Tabela 4.5 – (i) palavra-chave; (ii) texto comum; (iii) texto cifrado.

(i)	S	A	M	A	E	L	S	A	M	A	E	L	S	A	M	A	E	L	S	A
(ii)	c	r	i	p	t	o	g	r	a	f	i	a	r	e	v	e	l	a	d	a
(iii)	U	R	U	P	X	Z	Y	R	M	F	M	L	J	E	H	E	P	L	V	A

Fonte: Elaborado pelo autor.

Na Tabela 4.5, temos a frase a ser criptografada na segunda linha e, na primeira linha, a palavra-chave repetida várias vezes para acompanhar o tamanho da frase da segunda linha, e truncada ao final.

Para criptografar a primeira letra, **c**, começamos identificando a letra-chave acima dela, **S**, que por sua vez define uma linha particular no quadrado de Vigenère. A linha que começa com **S**, linha 18, é o alfabeto cifrado que vamos usar para encontrar a letra substituta para o texto comum **c**. Olhamos para ver onde a coluna encabeçada por **c** cruza-se com a linha 18, iniciada com **S**, interseção que acaba sendo a letra **U**. Consequentemente, a letra **c** no texto comum é representada por **U** no texto cifrado.

Para cifrar a segunda letra da mensagem, **r**, o processo é repetido. A letra da chave acima de **r** é **A**, então **é** criptografado por meio da que se inicia com A no quadrado de Vigenère: a linha 26, que é um novo alfabeto cifrado (neste caso idêntico ao alfabeto a ser cifrado). Por isso **r** torna-se **R**. Para criptografar **i**, olhamos para ver onde a coluna encabeçada por **i** cruza a linha começando com **M**, que acaba sendo a letra **U**. Consequentemente, a letra **i** no o texto comum é representada por **U** no texto cifrado. Cada letra da palavra-chave indica um determinado alfabeto cifrado dentro do Quadrado de Vigenère, e como a palavra-chave contém seis letras, o remetente criptografa a mensagem percorrendo seis linhas do Quadrado de Vigenère. A sexta letra da mensagem é cifrada de acordo com a sexta letra da palavra-chave, L, mas para cifrar a sétima letra da mensagem temos que retornar à primeira letra da palavra-chave.

A cifra de Vigenère pode ser vista algebricamente, da seguinte maneira.

Inicialmente consideremos cada letra $\mathrm{P_i}$ do alfabeto original com sua relação numérica ℓ_i dada na Tabela 4.4, trabalhando novamente na aritmética módulo 26 a criptografia pode ser dada pela fórmula,

$$\mathrm{C_i} = \mathrm{P_i} + \ell_i \pmod{26}.$$

A decriptação dada pela fórmula,

$$\mathrm{C_i} = \mathrm{P_i} - \ell_i + 26 \pmod{26},$$

$\mathrm{C_i}$ representa uma letra do alfabeto cifrado.

Para clarear as fórmulas acima, podemos algebrizar (ou aritmetizar) a cifra de Vigenère usando a Tabela 4.2, que reproduzimos aqui na Tabela 4.6.

Tabela 4.6 – Cifra de César traduzida em números.

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

Fonte: Elaborado pelo autor.

Pela Tabela 4.6, a palavra-chave SAMAEL fica associada a uma sequência $(18, 26, 12, 26, 4, 11)$ que é reproduzida indefinidamente quantas vezes for necessário, dependendo do tamanho do texto a ser cifrado.

Pela Tabela 4.6, a mensagem **criptografia revelada** é então associado à sequência

$$\mathrm{m} = (2, 17, 8, 15, 19, 14, 6, 17, 26, 5, 8, 26, 17, 4, 21, 4, 11, 26, 3, 26)$$

Por repetições de chave SAMAEL, a chave k para criptografar a mensagem será então

$$\mathrm{k} = (18, 26, 12, 26, 4, 11, 18, 26, 12, 26, 4, 11, 18, 26, 12, 26, 4, 11, 18, 26)$$

A mensagem cifrada será então dada pela soma $\mathrm{c} = \mathrm{m} + \mathrm{k}$, módulo 26, coordenada a coordenada.

Para facilitar a compreensão colocaremos mensagem e chave em correspondência nas colunas, com respectivas somas na terceira linha.

2	17	8	15	19	14	6	17	26	5	8	26	17	4	21	4	11	26	3	26
18	26	12	26	4	11	18	26	12	26	4	11	18	26	12	26	4	11	18	26
20	17	20	15	23	25	24	17	12	5	12	11	9	4	7	4	15	11	21	26

Assim temos a mensagem cifrada dada por

$$\mathrm{c} = (20, 17, 20, 15, 23, 25, 24, 17, 12, 5, 12, 11, 9, 4, 7, 4, 15, 11, 21, 26)$$

que corresponde à sequência de letras **URUPXZYRMFMLJEHEPLVA**.

Para ter a mensagem revelada, o receptor deverá aplicar a chave $\mathrm{k}' = -\mathrm{k}$ módulo 26 à mensagem cifrada, sendo então $\mathrm{k}' = (8, 26, 14, 26, 22, 15)$, repetida indefinidamente de acordo com a mensagem cifrada recebida.

O receptor calcula então $\mathrm{c} + \mathrm{k}'$ módulo 26,

20	17	20	15	23	25	24	17	12	5	12	11	9	4	7	4	15	11	21	26
8	26	14	26	22	15	8	26	14	26	22	15	8	26	14	26	22	15	8	26
2	17	8	15	19	14	6	17	26	5	8	26	17	4	21	4	11	26	3	26

e obtém como resultado

$$\mathrm{c} + \mathrm{k}' = (2, 17, 8, 15, 19, 14, 6, 17, 26, 5, 8, 26, 17, 4, 21, 4, 11, 26, 3, 26) = \mathrm{m}$$

a qual, pela codificação dada pela Tabela 4.6, corresponderá à frase **criptografiarevelada**.

4.3 CIFRAS DE HILL

A referência básica e principal utilizada para o desenvolvimento desta seção é (ANTON; RORRES, 2012).

Um *sistema poligráfico* é um sistema de criptografia no qual o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas. Nesta seção, estudamos uma classe de sistemas poligráficos conhecidos como *cifras de Hill*, que têm por base transformações matriciais. O nome é em referência a Lester S. Hill, que introduziu esses sistemas em dois trabalhos, *Cryptography in an Algebraic Alphabet*, American Mathematical Monthly, Vol. 36, junho-julho de 1929, páginas 306-312 e *Concerning Certain Linear Transformation Apparatus of Cryptography*, American Mathematical Monthly, Vol. 38, março de 1931, páginas 135-154, (ANTON; RORRES, 2012).

Nesta seção, vamos supor que cada letra de texto comum e de texto cifrado,

excetuando-se a letra Z, tem um valor numérico que especifica sua posição no alfabeto padrão conforme a Tabela 4.7. Por motivos que ficarão claros adiante, damos a Z o valor de 0.

Tabela 4.7 – Alfabeto com valores numéricos para a cifra de Hill.

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	0

Fonte: Elaborado pelo autor.

Nos casos mais simples de cifras de Hill, transformamos pares sucessivos de letras no texto comum em texto cifrado segundo o procedimento seguinte.

(Passo 1) Escolhemos uma matriz A de ordem 2, $A \neq I_2$, de coeficientes inteiros e inversível módulo 26, denominada *matriz cifradora* A, que terá uma forma

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}; \quad a_{ij} \in \mathbb{Z}_{26}.$$

(Passo 2) Agrupamos pares de letras consecutivas do *texto comum*, adicionando uma *letra adicional fictícia* para completar o último par se o texto comum tiver um número ímpar de letras, e substituímos cada letra de texto comum por seu valor numérico.

(Passo 3) Cada par (p_1, p_2) de números associados a pares de letras é convertido em um vetor coluna

$$\vec{p} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$

e formamos o produto $A \cdot \vec{p}$.

Dizemos que $\vec{p}$ é o *vetor comum* e $A \cdot \vec{p} = \vec{c}$, o correspondente *vetor cifrado*.

(Passo 4) Convertemos cada vetor cifrado em seu equivalente alfabético.

Exemplo 4.1. Codifiquemos a mensagem *SECRETOS*. Para isto devemos transformar pares sucessivos das letras do texto comum em texto cifrado seguindo a Tabela 4.7.

S	E	C	R	E	T	O	S
19	5	3	18	5	20	15	19

Agora convertemos cada par sucessivo de números associados em um vetor coluna,

$$\mathrm{SE} \leftrightarrow \begin{pmatrix} 19 \\ 5 \end{pmatrix} \quad \mathrm{CR} \leftrightarrow \begin{pmatrix} 3 \\ 18 \end{pmatrix} \quad \mathrm{ET} \leftrightarrow \begin{pmatrix} 5 \\ 20 \end{pmatrix} \quad \mathrm{OS} \leftrightarrow \begin{pmatrix} 15 \\ 19 \end{pmatrix}.$$

Adotaremos a matriz $A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ como matriz cifradora. Notemos que A é inversível módulo 26, pois $\det(A) = 3$ tem inverso multiplicativo em $\mathbb{Z}_{26}$, propriedade que estabeleceremos adiante de modo mais geral no Teorema 4.1.

Para codificar o par SE, efetuamos o produto matricial

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 19 \\ 5 \end{pmatrix} = \begin{pmatrix} 29 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 15 \end{pmatrix} \pmod{26}.$$

Para codificar o par CR, efetuamos o produto matricial

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 18 \end{pmatrix} = \begin{pmatrix} 39 \\ 54 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 2 \end{pmatrix} \pmod{26}.$$

Para codificar o par ET, efetuamos o produto matricial

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 5 \\ 20 \end{pmatrix} = \begin{pmatrix} 45 \\ 60 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 8 \end{pmatrix} \pmod{26}.$$

Para codificar o par OS, efetuamos o produto matricial

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 15 \\ 19 \end{pmatrix} = \begin{pmatrix} 53 \\ 57 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 5 \end{pmatrix} \pmod{26}.$$

Então a partir dos vetores cifrados $\begin{pmatrix} 3 \\ 15 \end{pmatrix}, \begin{pmatrix} 13 \\ 2 \end{pmatrix}, \begin{pmatrix} 19 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 5 \end{pmatrix}$, obtemos a mensagem cifrada COMBSHAE.

Exemplo 4.2. Codifiquemos a mensagem *VACINAS*, para tanto, adicionamos a letra fictícia W para completarmos o último par. Novamente seguindo a Tabela 4.7 obtemos a associação

V	A	C	I	N	A	S	W
22	1	3	9	14	1	19	23

.

Agora convertemos os pares sucessivos de números associados s pares de letras em vetores colunas,

$$VA \leftrightarrow \begin{pmatrix} 22 \\ 1 \end{pmatrix} \quad CI \leftrightarrow \begin{pmatrix} 3 \\ 9 \end{pmatrix} \quad NA \leftrightarrow \begin{pmatrix} 14 \\ 1 \end{pmatrix} \quad SW \leftrightarrow \begin{pmatrix} 19 \\ 23 \end{pmatrix}.$$

Adotaremos a matriz $A = \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}$ como matriz cifradora.

Para codificar o par VA, efetuamos o produto matricial

$$\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 22 \\ 1 \end{pmatrix} = \begin{pmatrix} 23 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} 23 \\ 3 \end{pmatrix} \pmod{26}.$$

Para codificar o par CI, efetuamos o produto matricial

$$\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 9 \end{pmatrix} = \begin{pmatrix} 12 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 1 \end{pmatrix} \pmod{26}.$$

Para codificar o par NA, efetuamos o produto matricial

$$\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 14 \\ 1 \end{pmatrix} = \begin{pmatrix} 15 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 3 \end{pmatrix} \pmod{26}.$$

Para codificar o par SW, efetuamos o produto matricial

$$\begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 19 \\ 23 \end{pmatrix} = \begin{pmatrix} 42 \\ 69 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 17 \end{pmatrix} \pmod{26}.$$

Então a partir dos vetores cifrados $\begin{pmatrix} 23 \\ 3 \end{pmatrix}, \begin{pmatrix} 12 \\ 1 \end{pmatrix}, \begin{pmatrix} 15 \\ 3 \end{pmatrix}, \begin{pmatrix} 16 \\ 17 \end{pmatrix}$, obtemos a mensagem cifrada WCLAOCPQ.

Como o texto comum foi subdividido em pares de letras e criptografado por uma matriz 2×2, dizemos que a cifra de Hill do Exemplo 4.2 é uma cifra de Hill de ordem 2. Evidentemente, também é possível agrupar o texto comum em ternos e criptografar com uma matriz 3×3 de entradas inteiras, obtendo uma **cifra de Hill de ordem 3**. Em geral, para uma **cifra de Hill de ordem n**, subdividimos o texto comum em conjuntos de n letras e codificamos os blocos com uma **matriz codificadora** $n \times n$ de entradas inteiras, inversível módulo 26, e diferente da matriz I_n.

Cada cifra útil deve possuir um procedimento para decifração. Para decifrar as cifras de Hill, usamos a inversa módulo 26 da matriz codificadora. Para ser preciso, se m for

um inteiro positivo, dizemos que uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é inversível módulo m se existir uma matriz B com entradas em $\mathbb{Z}_m$ tal que

$$AB = BA = I \pmod{m}.$$

Suponhamos, agora, que

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

seja inversível módulo 26 e que essa matriz seja usada numa cifra de Hill de ordem 2. Se

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$

é um vetor comum, então

$$c = A\mathbf{p} \pmod{26}$$

é o correspondente vetor cifrado e

$$\mathbf{p} = A^{-1}c \pmod{26}.$$

Assim, cada vetor comum pode ser recuperado do correspondente vetor cifrado pela multiplicação à esquerda por $A^{-1} \pmod{26}$. Na criptografia, é importante saber quais matrizes são invertíveis módulo 26 e como obter suas inversas. Passamos a investigar essas questões. Na aritmética comum das matrizes reais, uma matriz quadrada A é inversível se, e somente se, $\det(A) \neq 0$ ou, equivalentemente, $\det(A)$ tem um inverso multiplicativo. O teorema seguinte é o análogo desse resultado em aritmética modular.

Teorema 4.1. *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é inversível módulo m se, e somente se, o resíduo de $\det(A)$ módulo m tem um recíproco (inverso multiplicativo) módulo m.*

A demonstração do Teorema 4.1, no caso de matrizes 2×2, é análoga àquela feita para o Teorema 3.2.

Como o resíduo de $\det(A)$ módulo m tem um recíproco módulo m se, e somente se, esse resíduo e m não têm fator primo comum, obtemos o corolário seguinte.

Corolário 4.1. *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é inversível módulo m se, e*

somente se, m e o resíduo de $\det(A)$ *módulo* m *não têm fatores primos comuns, ou seja,* $\mathrm{mdc}(m, \det(A)) = 1$.

Como os únicos fatores primos de $m = 26$ são 2 e 13, obtemos o corolário seguinte, que é útil para as cifras de Hill.

Corolário 4.2. *Uma matriz quadrada* A *com entradas em* $\mathbb{Z}_{26}$ *é inversível módulo* 26 *se, e somente se, o resíduo de* $\det(A)$ *módulo* 26 *não é divisível por* 2 *e nem por* 13.

Se usarmos o Teorema 4.1 com a Definição 3.15 podemos calcular a inversa de uma matriz 2×2 módulo 26 como segue.

Seja $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ com $a_{11}, a_{12}, a_{21}, a_{22} \in \mathbb{Z}_{26}$, se o resíduo de $\det(A) = a_{11}a_{22} - a_{21}a_{12}$ módulo 26 não for divisível por 2 e nem por 13, então a inversa de $A \pmod{26}$ será dada por

$$A^{-1} = (\det(A))^{-1} \begin{pmatrix} a_{22} & 26 - a_{12} \\ 26 - a_{21} & a_{11} \end{pmatrix} \pmod{26}$$

sendo $(\det(A))^{-1}$ é o recíproco do resíduo de $\det(A) \pmod{26}$.

Exemplo 4.3 (**Decifragem de uma Cifra de Hill de ordem 2**).

Vamos agora decifrar a mensagem cifrada dada no Exemplo 4.2, WCLAOCPQ.

Pela Tabela 4.7, o equivalente numérico do texto cifrado é

$$23 \quad 3 \qquad 12 \quad 1 \qquad 15 \quad 3 \qquad 16 \quad 25$$

.

A matriz cifradora usada foi $A = \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}$, e sua inversa módulo 26 é

$$A^{-1} = \begin{pmatrix} 1 & 17 \\ 0 & 9 \end{pmatrix} \pmod{26}.$$

Para obtemos os pares do texto comum, multiplicamos cada par de texto cifrado pela inversa de A módulo 26, como segue.

$$\begin{pmatrix} 1 & 17 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} 23 \\ 3 \end{pmatrix} = \begin{pmatrix} 74 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 1 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 1 & 17 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} 12 \\ 1 \end{pmatrix} = \begin{pmatrix} 29 \\ 9 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 9 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 1 & 17 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} 15 \\ 3 \end{pmatrix} = \begin{pmatrix} 66 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 1 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 1 & 17 \\ 0 & 9 \end{pmatrix} \begin{pmatrix} 16 \\ 17 \end{pmatrix} = \begin{pmatrix} 305 \\ 153 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 23 \end{pmatrix} \pmod{26}$$

Pela Tabela 4.7, os equivalentes alfabéticos destes vetores são

$$V \quad A \qquad C \quad I \qquad N \quad A \qquad S \quad W$$

que fornecem a mensagem VACINASW.

Como o objetivo de criptografar mensagens e informações e impedir que “oponentes” descubram seu conteúdo, os criptógrafos têm uma preocupação com a segurança de suas cifras, ou seja, sobre quão facilmente suas mensagens cifradas podem ser decifradas (ou quebradas) pelos oponentes. Concluímos esta seção discutindo uma técnica para quebrar cifras de Hill.

Suponha que consigamos algum texto comum e o cifrado correspondente de uma mensagem de nosso oponente. Por exemplo, digamos que, examinando algum texto cifrado interceptado, fomos capazes de deduzir que a mensagem é uma carta que começa com CARO DETETIVE.

Mostremos que, com alguns poucos desses dados, pode ser possível determinar a matriz decodificadora de uma cifra de Hill e, consequentemente, ter acesso ao resto da mensagem. É um resultado básico em Álgebra Linear que uma transformação fica completamente determinada por seus valores numa base.

Esse princípio sugere que, se tivermos uma cifra de Hill de ordem n e se

$$p_1,\ p_2, \ldots,\ p_n$$

forem vetores comuns “linearmente independentes” cujos correspondentes vetores cifrados

$$Ap_1,\ Ap_2, \ldots,\ Ap_n$$

sejam conhecidos, então disporemos de informação suficiente para determinar a matriz A e, portanto, sua inversa $A^{-1} \pmod{m}$.

O próximo teorema, que enunciaremos sem demonstrar, fornece uma maneira de fazer isso.

Teorema 4.2 (Determinando a matriz decodificadora)**.** *Sejam $p_1, p_2, \ldots, p_n$ vetores comuns linearmente independentes e sejam $c_1, c_2, \ldots, c_n$ os correspondentes vetores cifrados de uma cifra de Hill de ordem n (cuja matriz cifradora é $n \times n$). Se*

$$P = \begin{bmatrix} p_1^T \\ p_2^T \\ \vdots \\ p_n^T \end{bmatrix}$$

for a matriz $n \times n$ de vetores colunas $p_1^T,\ p_2^T, \ldots,\ p_n^T$ e se

$$C = \begin{bmatrix} c_1^T \\ c_2^T \\ \vdots \\ c_n^T \end{bmatrix}$$

for a matriz $n \times n$ de vetores linha $c_1^T,\ c_2^T, \ldots,\ c_n^T$, então a sequência de operações elementares com as linhas que reduz C a I transforma P em $(A^{-1})^T$.

Esse teorema nos diz que, para encontrar a transposta da matriz decodificadora A^{-1}, devemos encontrar uma sequência de operações elementares com as linhas que reduza C a I e então aplicar essas mesmas operações com as linhas de P. O próximo exemplo ilustra um algoritmo simples para fazer isso.

Exemplo 4.4 (Usando o Teorema 4.2)**.** Foi interceptada a cifra de Hill de ordem 2

$$\text{CFRKDSTITUVK}$$

Vamos decifrar essa mensagem, sabendo que ela começa com a palavra $CARO$.

Solução. Pela Tabela 4.7, o equivalente numérico do texto conhecido é

C	A	R	O
3	1	18	15

e o equivalente numérico do texto cifrado é

$$\begin{matrix} C & F & R & K \\ 3 & 6 & 18 & 11 \end{matrix}$$

de modo que os vetores comuns e correspondentes vetores cifrados são

$$p_1 = \begin{bmatrix} 3 \\ 1 \end{bmatrix} \leftrightarrow c_1 = \begin{bmatrix} 3 \\ 6 \end{bmatrix}, \qquad p_2 = \begin{bmatrix} 18 \\ 15 \end{bmatrix} \leftrightarrow c_2 = \begin{bmatrix} 18 \\ 11 \end{bmatrix}.$$

Queremos reduzir

$$C = \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix} = \begin{bmatrix} 3 & 6 \\ 18 & 11 \end{bmatrix}$$

a I por operações elementares com as linhas e, simultaneamente, aplicar essas operações a

$$P = \begin{bmatrix} p_1^T \\ p_2^T \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 18 & 15 \end{bmatrix}$$

para obter $(A^{-1})^T$ (a transposta da matriz decodificadora). Isso pode ser obtido adjuntando P à direita de C e aplicando as operações com as linhas à matriz resultante $[C \mid P]$ até que o lado esquerdo esteja reduzido a I. A matriz final, então, terá o formato $[I|(A^{-1})^T]$. As

contas podem ser feitas como segue

$$
\begin{aligned}
&\left[\begin{array}{cc|cc} 3 & 6 & 3 & 1 \\ 18 & 11 & 18 & 15 \end{array}\right] \quad \left((\mathcal{L}_1 \cdot 3^{-1} = \mathcal{L}_1 \cdot 9) \to \mathcal{L}_1\right) \\
\sim &\left[\begin{array}{cc|cc} 27 & 54 & 27 & 9 \\ 18 & 11 & 18 & 15 \end{array}\right] \quad (\mathcal{L}_1 \pmod{26} \to \mathcal{L}_1) \\
\sim &\left[\begin{array}{cc|cc} 1 & 2 & 1 & 9 \\ 18 & 11 & 18 & 15 \end{array}\right] \quad ((-18\mathcal{L}_1 + \mathcal{L}_2) \to \mathcal{L}_2) \\
\sim &\left[\begin{array}{cc|cc} 1 & 2 & 1 & 9 \\ 0 & -25 & 0 & -147 \end{array}\right] \quad (\mathcal{L}_2 \pmod{26} \to \mathcal{L}_2) \\
\sim &\left[\begin{array}{cc|cc} 1 & 2 & 1 & 9 \\ 0 & 1 & 0 & 9 \end{array}\right] \quad (-2\mathcal{L}_2 + \mathcal{L}_1) \to \mathcal{L}_1) \\
\sim &\left[\begin{array}{cc|cc} 1 & 0 & 1 & -9 \\ 0 & 1 & 0 & 9 \end{array}\right] \quad (\mathcal{L}_1 \pmod{26} \to \mathcal{L}_1) \\
\sim &\left[\begin{array}{cc|cc} 1 & 0 & 1 & 17 \\ 0 & 1 & 0 & 9 \end{array}\right]
\end{aligned}
$$

Assim,

$$(A^{-1})^T = \begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}$$

e, portanto, a matriz decodificadora é

$$A^{-1} = \begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix}.$$

Para decifrar a mensagem, agrupamos primeiro o texto cifrado em pares e encontramos os equivalentes numéricos de cada letra, como segue.

C	F	R	K	D	S	T	I	T	U	V	K
3	6	18	11	4	19	20	9	20	21	22	11

Em seguida, multiplicamos os vetores cifrados sucessivamente pela esquerda por A^{-1} e encontramos os equivalentes alfabéticos dos pares de texto comum resultantes.

$$\begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 3 \\ 6 \end{bmatrix} = \begin{bmatrix} 3 \\ 105 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 1 \end{bmatrix} \pmod{26} \quad \leftrightarrow \quad CA$$

$$\begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 18 \\ 11 \end{bmatrix} = \begin{bmatrix} 18 \\ 405 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 15 \end{bmatrix} \pmod{26} \quad \leftrightarrow \quad \text{RO}$$

$$\begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 4 \\ 19 \end{bmatrix} = \begin{bmatrix} 4 \\ 239 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 5 \end{bmatrix} \pmod{26} \quad \leftrightarrow \quad \text{DE}$$

$$\begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 20 \\ 9 \end{bmatrix} = \begin{bmatrix} 20 \\ 421 \end{bmatrix} \equiv \begin{bmatrix} 20 \\ 5 \end{bmatrix} \pmod{26} \quad \leftrightarrow \quad \text{TE}$$

$$\begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 20 \\ 21 \end{bmatrix} = \begin{bmatrix} 20 \\ 529 \end{bmatrix} \equiv \begin{bmatrix} 20 \\ 9 \end{bmatrix} \pmod{26} \quad \leftrightarrow \quad \text{TI}$$

$$\begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix} \begin{bmatrix} 22 \\ 11 \end{bmatrix} = \begin{bmatrix} 22 \\ 473 \end{bmatrix} \equiv \begin{bmatrix} 22 \\ 5 \end{bmatrix} \pmod{26} \quad \leftrightarrow \quad \text{VE}$$

Finalmente, construímos a mensagem a partir dos pares de texto comum:

CA RO DE TE TI VE

CARODETETIVE

4.3.1 Contando as cifras de Hill de ordem 2

Outro fato interessante, que temos com as cifras de Hill, é o número possível de chaves (matrizes cifradoras de ordem 2) distintas que podemos criar.

Os fatos aqui citados foram coletados através de consulta às referências (2850514, acesso em 26/06/2021) e (OLSAVSKY, 1990). São apenas enunciados e tratados sem demonstrações, envolvendo conceitos de álgebra clássica de anéis e grupos.

Seja $\mathcal{A} = \{A \in M_{2\times 2}(\mathbb{Z}_{26}) \mid \exists A^{-1} \pmod{26}\}$. O número de elementos de $\mathcal{A}$ pode ser calculado através do *Teorema Chinês dos Restos*, ou seja, uma matriz $A_{2\times 2}$ é inversível módulo 26 se for inversível módulo 2 e inversível módulo 13.

Na literatura de teoria dos grupos, o conjunto $\mathcal{A}$ é denotado por $\mathrm{GL}(2, \mathbb{Z}_{26})$, assim como é usada a notação $\mathrm{GL}(2, \mathbb{Z}_p)$ para denotar o conjunto (grupo) das matrizes 2×2 inversíveis módulo p.

Sendo p primo, o número de elementos de $\mathrm{GL}(2, \mathbb{Z}_p)$ é dado por

$$|\mathrm{GL}(2, \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p) \tag{4.1}$$

O *Teorema Chinês dos Restos* nos garante que

$$\mathbb{Z}_{26} \cong \mathbb{Z}_2 \times \mathbb{Z}_{13}$$

em termos de isomorfismo de anéis, e isto induz um isomorfismo de grupos

$$\mathrm{GL}(2, \mathbb{Z}_{26}) \cong \mathrm{GL}(2, \mathbb{Z}_2 \times \mathbb{Z}_{13}) \cong \mathrm{GL}(2, \mathbb{Z}_2) \times \mathrm{GL}(2, \mathbb{Z}_{13})$$

O número de elementos de $\mathrm{GL}(2, \mathbb{Z}_{26})$ é dado por

$$|\mathrm{GL}(2, \mathbb{Z}_{26})| = |\mathrm{GL}(2, \mathbb{Z}_2)| \cdot |\mathrm{GL}(2, \mathbb{Z}_{13})|$$

Precisamos então calcular $|\mathrm{GL}(2, \mathbb{Z}_2)|$ e $|\mathrm{GL}(2, \mathbb{Z}_{13})|$, pela igualdade (4.1).

$$|\mathrm{GL}(2, \mathbb{Z}_2)| = (2^2 - 1)(2^2 - 2) = 3 \cdot 2 = 6$$

$$|\mathrm{GL}(2, \mathbb{Z}_{13})| = (13^2 - 1)(13^2 - 13) = 168 \cdot 156 = 26208$$

Daí $|\mathrm{GL}(2, \mathbb{Z}_{26})| = |\mathrm{GL}(2, \mathbb{Z}_2)| \cdot |\mathrm{GL}(2, \mathbb{Z}_{13})| = 6 \cdot 26208 = 157248$

Portanto, excluindo-se a matriz I_2, 157247 é o número possível de chaves distintas de ordem 2.

4.4 CRIPTOGRAFIA DE CHAVE PÚBLICA

Para a redação desta seção e da próxima foram consultados, no que diz respeito a aspectos históricos, (SINGH, 2001a) e (SINGH, 2001b). Para a redação dos aspectos matemáticos foram consultados (SHOKRANIAN, 2005) e (COUTINHO, 2015).

Os criptossistemas que discutimos até agora são todos exemplos de criptossistemas de chave privada, ou simétrica, criptossistemas onde as chaves de criptografia e descriptografia são iguais ou podem ser facilmente encontrados um do outro. Por exemplo, em uma cifra de deslocamento, como a cifra de César, a chave de criptografia é um inteiro k e a chave de descriptografia correspondente é o inteiro $-\mathrm{k}$. Em uma cifra afim, chave de criptografia é um par (a, b) de inteiros e a chave de descriptografia correspondente é o par $(\bar{\mathrm{a}}, -\bar{\mathrm{a}}\mathrm{b})$ sendo $\bar{\mathrm{a}}$ o inverso de a módulo 26. Em uma cifra de Hill, a chave de criptografia é uma matriz A $_{\mathrm{n}\times\mathrm{n}}$ e a chave de descriptografia correspondente é a matriz $\bar{\mathrm{A}}_{\mathrm{n}\times\mathrm{n}}$, sendo $\bar{\mathrm{A}}$ a inversa da matriz A módulo 26.

Por esse motivo, se um dos criptossistemas discutidos até agora é usado para estabelecer comunicações seguras dentro de uma rede, então cada par de comunicantes

deve empregar uma chave de criptografia que é mantida em segredo para outras pessoas na rede, porque uma vez que a chave de criptografia em tal sistema de criptografia é conhecida, a chave de descriptografia pode ser encontrada usando uma pequena quantidade de tempo computacional. Consequentemente, para manter o sigilo, as chaves devem ser transmitidas por um canal de comunicação segura.

Para evitar atribuir uma chave a cada par de indivíduos, a qual deve ser mantida em segredo do resto da rede, um novo tipo de criptossistema, chamado criptossistema de chave pública, foi inventado na década de 1970. Nesse tipo de sistema de criptografia, as chaves de criptografia podem ser tornadas públicas, porque uma quantidade irrealística de grande tempo computacional é necessária para encontrar uma transformação de descriptografia através de uma transformação de criptografia.

Para usar um criptossistema de chave pública afim de estabelecer comunicações secretas em uma rede de indivíduos, cada indivíduo produz uma chave do tipo especificado pelo criptossistema, retendo certas informações privadas que entram na construção da transformação de criptografia E_k, obtida a partir da chave k de acordo com uma regra especificada. Em seguida, um diretório com chaves $k_1, k_2, \ldots, k_n$ é publicado. Quando o indivíduo i deseja enviar uma mensagem ao indivíduo j, as letras da mensagem são transformadas em seus equivalentes numéricos e combinados em blocos de tamanho específico. Então, para cada bloco de texto simples P, um bloco de texto cifrado correspondente $C = E_{k_j}(P)$, calculado usando a transformação de criptografia E_{k_j}. Para descriptografar a mensagem, individualmente, o receptor j aplica a transformação de descriptografia D_{k_j} em cada bloco de texto cifrado C para encontrar P, isto é,

$$D_{k_j}(C) = D_{k_j}(E_{k_j}(P)) = P.$$

Como a transformação de descriptografia D_{k_j} não pode ser encontrada em um período de tempo real por qualquer pessoa que não seja o indivíduo j, nenhum indivíduo não autorizado pode descriptografar a mensagem, embora seja conhecida a chave k_j. A criptoanálise da mensagem do texto cifrado, mesmo com conhecimento de k_j, é extremamente inviável devido à grande quantidade de tempo de cálculo necessário.

Muitos criptossistemas foram propostos como sistemas criptográficos de chave pública. Todos, exceto alguns, se mostraram inadequados, demonstrando que as mensagens de texto cifrado poderiam ser descriptografadas usando uma quantidade viável de tempo de computador.

Nesta próxima seção, apresentaremos o criptossistema de chave pública amplamente usado, o **criptossistema RSA**.

4.5 CRIPTOGRAFIA RSA

Para descrição do funcionamento da criptografia RSA, consideraremos, através de simplificações necessárias a uma exposição didática, uma outra tabela relacionando números e letras, para não causar ambiguidade na decifração da mensagem criptografada. A nova tabela relacionando números e letras é dada a seguir.

Tabela 4.8 – Letras e seus valores numéricos para uma criptografia RSA.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Elaborado pelo autor.

Um criptossistema de chave pública comumente usado tem sido o criptossistema RSA, cuja sigla se refere aos sobrenomes de seus criadores, *Ronald Rivest*, *Adi Shamir* e *Leonard Adleman*, que o descreveram em uma publicação de 1977.

No entanto, este criptossistema havia sido realmente inventado vários anos antes, em 1973, pelo matemático britânico Clifford Cocks em um trabalho secreto na Sede de Comunicações da inteligência britânica. A invenção de Cocks foi mantida em sigilo pelo governo britânico e tornou-se pública em 1997.

O criptossistema RSA é um criptossistema de chave pública baseado em exponenciação modular, onde a chave de codificação é um par (e, n) consistindo em um expoente e e um módulo n que é o produto de dois grandes números primos, ou seja, $n = p \cdot q$, onde p e q são números primos grandes adequadamente escolhidos, sendo $e > 1$ e $\mathrm{mdc}(e, \varphi(n)) = 1$.

Para criptografar uma mensagem, primeiro relacionamos as letras com seus números equivalentes (de acordo com a Tabela 4.8) e, em seguida, formamos blocos do maior tamanho possível (com um número par de dígitos). Para criptografarmos um bloco de texto comum P, aplicamos a transformação de criptografia $E(P)$ para obtermos o bloco de texto cifrado C, sendo

$$E(P) = C \equiv P^e \pmod{n}, \qquad 0 \leq C < n.$$

O procedimento de *descriptografia* requer conhecimento de um inverso d de e módulo $\varphi(n)$, que existe porque $\mathrm{mdc}(e, \varphi(n)) = 1$. Para descriptografar o bloco de texto cifrado C, a transformação de descriptografia D aplicada a C é da forma

$$D(C) \equiv P^d \pmod{n}, \qquad 0 \leq D(C) < n.$$

Para termos $D(C) = (P^e)^d = P \pmod{n}$ para todas as mensagens de texto simples P possíveis, observemos que $ed \equiv 1 \pmod{\varphi(n)}$, logo $ed = k\varphi(n) + 1$ para algum inteiro k. Temos então

$$D(C) = C^d = (P^e)^d = P^{ed} \equiv P^{k\varphi(n)+1} \equiv P^{k\varphi(n)} \cdot P \pmod{n}.$$

Se os fatores primos de n são suficientemente grandes, teremos $\mathrm{mdc}(P, n) = 1$. Pelo teorema de Euler sabemos que então $P^{\varphi(n)} \equiv 1 \pmod{n}$.

Logo

$$P^{\varphi(n)k}P \equiv (P^{\varphi(n)})^k P \equiv 1^k \cdot P = P \pmod{n}.$$

Portanto

$$D(C) \equiv P \pmod{n}.$$

Assim sendo, para o criptossistema RSA, sendo d o inverso de e módulo $\varphi(n)$, o par (d, n) será a chave de descriptografia correspondente à chave de criptografia (e, n).

4.5.1 Um exemplo simplificado de criptografia RSA

Para ilustrarmos como o criptossistema RSA funciona, suponhamos que o módulo de criptografia seja o produto dos dois primos 43 e 59 (que são menores que os grandes números primos que seriam realmente usados); assim, temos $43 \cdot 59 = 2537$ como o módulo. Tomamos $e = 13$ como o expoente; notemos que $\mathrm{mdc}(e, \varphi(n)) = \mathrm{mdc}(13, 42 \cdot 58) = 1$. Para criptografar a mensagem

PASSAGEM SECRETA

Inicialmente adicionamos a letra fictícia W no final da mensagem, isto para obtermos um número par de letras. Em seguida, transformamos as letras em seus equivalentes

numéricos, e então agrupamos esses números juntos em blocos de quatro. Obtendo a mensagem de texto comum

$$1500 \quad 1818 \quad 0006 \quad 0412$$
$$1804 \quad 0217 \quad 0419 \quad 0022$$

Criptografamos cada bloco P de texto comum em um bloco C de texto cifrado, usando a relação

$$C \equiv P^{13} \pmod{2537}.$$

Por exemplo, quando criptografamos o primeiro bloco de texto comum 1204, obtemos o bloco de texto cifrado

$$C \equiv 1500^{13} \equiv 784 \pmod{2537}.$$

Foi feito uso do programa Maple 12 para os cálculos de aritmética modular. A sintaxe para pedir o cálculo no programa é simplesmente da forma

```
[> 1500^13 mod 2537;
```

e o programa retorna, imediatamente,

```
784
```

Criptografando todos os blocos de texto comum, obtemos a mensagem de texto cifrado

$$0784 \quad 0949 \quad 2414 \quad 0412$$
$$1460 \quad 2410 \quad 0290 \quad 1570$$

Para descriptografar esta mensagem cifrada, devemos encontrar um inverso de $e = 13$ módulo $\varphi(2537) = \varphi(43 \cdot 59) = 42 \cdot 58 = 2436$. Então façamos o uso do Algoritmo Euclidiano para calcular o $\mathrm{mdc}(2436, 13)$, como segue.

$$\begin{array}{r|l} 2436 & 13 \\ \hline 5 & 187 \end{array} \qquad \begin{array}{r|l} 13 & 5 \\ \hline 3 & 2 \end{array} \qquad \begin{array}{r|l} 5 & 3 \\ \hline 2 & 1 \end{array} \qquad \begin{array}{r|l} 3 & 2 \\ \hline 1 & 1 \end{array}$$

Chamando $m = 2436$ e $e = 13$, isolamos os restos das divisões acima.
Da primeira divisão, temos que,

$$5 = m - 187e$$

Da segunda divisão, temos que,

$$3 = 13 - 2 \cdot 5 \Rightarrow 3 = e - 2(m - 187e) \Rightarrow 3 = -2m + 375e$$

Da terceira divisão, temos que,

$$2 = 5 - 3 \Rightarrow 2 = (m - 187e) - (-2m + 375e) \Rightarrow 2 = 3m - 562e$$

E da última divisão, temos que,

$$1 = 2 - 3 \Rightarrow 1 = (-2m + 375e) - (3m - 562e) \Rightarrow 1 = 937e - 5m$$

Logo $1 = 937e \pmod{m} \Rightarrow e^{-1} = 937 \pmod{m}$. O inverso de 13 módulo 2436 pode ser confirmado pelo Maple 12, pelas linha de comando

```
[> 13^(-1) mod 2436
```

que devolve 937.

Temos então que, $d = 937$ é o inverso de 13 módulo 2436. Consequentemente, para descriptografar cada bloco de texto cifrado C, usamos a relação

$$P \equiv C^{937} \pmod{2537}, \quad 0 \leq P < 2537,$$

que é válida porque

$$C^{937} \equiv (P^{13})^{937} \equiv (P^{2436})^5 P \equiv P \pmod{2537}.$$

Observe que usamos o teorema de Euler para termos

$$P^{\varphi(2537)} = P^{2436} \equiv 1 \pmod{2537},$$

quando $mdc(P, 2537) = 1$ (que vale para todos os blocos de texto comum neste exemplo).

4.5.2 Uma questão que não foi possível responder

No exemplo de criptografia RSA que foi explorando anteriormente, fizemos uso do módulo $m = 43 \cdot 59 = 2537$. Posteriormente calculamos $\varphi(m) = 2436$ e fizemos a transformação da mensagem PASSAGEM SECRETA, com o uso da Tabela 4.8, nos blocos de números

$$1500 \quad 1818 \quad 2371 \quad 0530$$
$$2343 \quad 0710 \quad 2017 \quad 0045$$

obtendo depois, através da transformação $C = P^{13} \pmod{2537}$ em cada bloco P, os blocos cifrados

$$0784 \quad 0949 \quad 2414 \quad 0412$$
$$1460 \quad 2410 \quad 0290 \quad 1570$$

Para decifrar a mensagem, em cada bloco cifrado C aplicamos a transformação $Q = C^{937}$, obtendo como resposta o correspondente bloco P da mensagem original. Como constatado, cada um dos blocos a ser cifrado é relativamente primo com m e portanto, pelo teorema 3.6 de Euler, $P^{\varphi(m)} \equiv 1 \pmod{m}$ e neste fato reside o sucesso do algoritmo.

No entanto, fizemos o experimento de usar blocos de quatro algarismos que poderiam ser blocos de mensagens, mas não relativamente primos com $2537 = 43 \cdot 59$. Por exemplo, ao criptografar a mensagem (sem sentido, mas possível) PFLSOQVY, traduziríamos, usando a Tabela 4.8, a mensagem nos blocos

$$1505 \quad 1118 \quad 1416 \quad 2124$$

Mas estes números de quatro algarismos não são primos com $m = 2537$, pois

$$1505 = 43 \cdot 35, \ 1118 = 43 \cdot 26, \ 1416 = 59 \cdot 24, \ 2124 = 59 \cdot 36.$$

Usando o programa Maple 12, foram feitos os cálculos

$$1505^{13} \equiv 1075 \pmod{2537}$$
$$1118^{13} \equiv 860 \pmod{2537}$$
$$1416^{13} \equiv 590 \pmod{2537}$$
$$2124^{13} \equiv 1475 \pmod{2537}$$

dando então como mensagem cifrada os blocos

$$1075 \quad 0860 \quad 0590 \quad 1475 \ .$$

Por um momento foi pensado que não seria possível recuperar os blocos de números da mensagem original, pois não temos mais as hipóteses que garantem o Teorema 3.6 de

Euler. No entanto, pelo Maple 12, são calculados

$$\begin{aligned} 1075^{937} &\equiv 1505 \pmod{2537} \\ 860^{937} &\equiv 1118 \pmod{2537} \\ 590^{937} &\equiv 1416 \pmod{2537} \\ 1475^{937} &\equiv 2124 \pmod{2537} \end{aligned}$$

que são precisamente os blocos da mensagem original, e no momento não temos nenhuma explicação matemática para o sucesso do resgate da mensagem original neste exemplo.

5 ATIVIDADES PARA SALA DE AULA

Já há vários trabalhos realizados, na forma de dissertações e/ou minicursos sugerindo atividades para a sala de aula envolvendo matemático do ensino básico e conceitos de criptografia. Dentre esses trabalhos citamos (MALAGUTTI, 2015) e (BEZERRA; MALAGUTTI; RODRIGUES, 2015).

Neste capítulo são sugeridas quatro atividades que podem ser realizadas em uma sala de aula do ensino médio, envolvendo cifras de César, cifras afins e a cifra de Vigenère.

A escrita em vermelho é um gabarito para o professor que decidir aplicar a atividade em sala de aula. O recomendado é deixar em branco para o aluno resolver. Folhas de atividades em branco são encontradas no apêndice deste trabalho.

Atividade 1. **A Cifra de César**

Júlio César usou uma cifra de substituição simples para enviar mensagens às suas tropas. Ele substituiu cada letra pela letra que estava 3 casas mais adiante no alfabeto, de modo que “A” foi substituído por “D”, “B” por “E” e assim por diante.

Questão 1. Complete a tabela abaixo para mostrar como cada letra é codificada usando este sistema.

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

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

Questão 2. Usando a Cifra de César, codifique o nome de seu país. Seu amigo obteve a mesma mensagem?

Questão 3. Decodifique esta mensagem, que foi codificada usando a cifra de César da tabela criada na **Questão 1**:

R	U	R	P	D	Q	R	D	F	D	W	D	D	P	R	U	H	V	D
O	R	O	M	A	N	O	A	C	A	T	A	A	M	O	R	E	S	A

G	D	P	D	V	D	P	D	G	D	V	H	U	R	P	D
D	A	M	A	S	A	M	A	D	A	S	E	R	O	M	A

D	W	D	F	D	R	Q	D	P	R	U	R
A	T	A	C	A	O	N	A	M	O	R	O

Atividade 2. **Cifra afim.**

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

a) Usando a função afim $f(x) = 2x + 3$, codifique a mensagem CRIPTOGRAFADA.

Primeiramente com a relação entre números e letras que foi dada obtemos:

(C, R, I, P, T, O, G, R, A, F, A, D, A) $\sim$ $(12, 27, 18, 25, 29, 16, 27, 36, 15, 36, 13, 36)$

Daí

$(12, 27, 18, 25, 29, 16, 27, 36, 15, 36, 13, 36) \overset{f}{\mapsto} (27, 57, 39, 53, 61, 35, 57, 75, 33, 75, 29, 75)$

e obtemos como mensagem codificada: 275739536135577533752975

b) Escreva uma mensagem e codifique-a usando a função $f(x) = 3x$.

Como exemplo de mensagem a ser codificada, considere a mensagem

BOM DIA

Neste caso temos a relação entre números e letras dada a seguir:

BOMDIA $\sim (11, 24, 22, 13, 18, 36)$

Daí

$(11, 24, 22, 13, 18, 36) \overset{f}{\longmapsto} (33, 72, 66, 39, 54, 108)$

Logo a mensagem codificada é 3372663954108.

c) Sabendo que a função cifradora é $f(x) = 2x + 1$, decodifique a mensagem:

$4529475773332945 \quad 57292555295973$

Como a função cifradora é $f(x) = 2x + 1$ para decodificar precisamos da função f^{-1}.

Cálculo da função f^{-1}:

$y = f(x) = 2x + 1 \Leftrightarrow f^{-1}(y) = 2^{-1}(y - 1)$

Considerando a mensagem codificada $4529475773332945 \quad 57292555295973$ podemos fazer a relação:

$(45, 29, 47, 57, 73, 33, 29, 45) \quad (57, 29, 25, 55, 29, 59, 73) \rightarrow$

$(45, 29, 47, 57, 73, 33, 29, 45, 57, 29, 25, 55, 29, 59, 73)$

Daí

$(45, 29, 47, 57, 73, 33, 29, 45, 57, 29, 25, 55, 29, 59, 73) \overset{f^{-1}}{\longmapsto}$
$(22, 14, 23, 28, 36, 16, 14, 22, 28, 14, 12, 27, 14, 29, 36)$

Temos a mensagem numérica $(22, 14, 23, 28, 36, 16, 14, 22)$ $(28, 14, 12, 27, 14, 29, 36)$

Usando a relação entre números e letras dada na tabela obtemos mensagem original:

MENSAGEM SECRETA

Atividade 3. **A Cifra de Vigenère.**

Esta é uma atividade a ser realizada em grupos de alunos.

Utilizando a tabela abaixo e a palavra chave **CUBO** codifique uma mensagem e depois envie-a a outro grupo, que deverá decifrá-la.

Tabela 5.1 – Quadrado de Vigenère

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

Atividade 4. **Tabelas Mágicas.**

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
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

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
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

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
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

i) Esta é uma atividade que pode ser realizada em duplas.

Codifique seu nome usando uma das cifras dadas nas tabelas acima. Peça ao seu amigo para descobrir qual chave você usou.

NOME: _____

Qual das tabelas mágicas foi usada nesta mensagem cifrada?

ii) Esta é uma atividade para ser realizada em equipes de quatro alunos.

Você e seus amigos estão planejando uma festa surpresa. Para garantir que ninguém mais descubra os detalhes, vocês irão codificá-los.

Cada um de vocês preencherá **UM** dos detalhes abaixo (decidam com antecedência quem fará qual parte). Codifique a resposta usando uma das tabelas acima (nem todos precisam usar a mesma tabela). Quando você terminar a codificação, entregue todos os seus papéis para uma outra equipe para ver se eles conseguem descobrir os detalhes da festa.

QUEM: (de quem é a festa surpresa?)

ONDE: (onde você vai dar a festa?)

DIVERSÃO: (que jogo ou atividade você fará para se divertir?)

PRESENTE: (que presente você vai trazer?)

6 CONSIDERAÇÕES FINAIS

O estudo de criptografia é excelente ferramenta para salientar aplicações da matemática básica, trazendo noções sobre o uso de funções afins, números inteiros e suas propriedades aritméticas, aritmética modular em nível introdutório. Além disso o uso de aritmética modular aplicada com álgebra matricial é um tópico fascinante na opinião do autor.

No trabalho de pesquisa para esta dissertação foi possível conhecer os aspectos históricos que envolvem criptografia tais o envio de mensagens secretas em tempos de guerra, e o uso da mesma em nosso cotidiano para fins pacíficos, por transações financeiras pela internet ou envio de mensagens secretas.

Sabemos que é necessária uma dedicação dos professores em buscar novos caminhos que tornem a aprendizagem mais significativa e é neste sentido que a Criptografia pode ser uma grande aliada na árdua tarefa do ensino-aprendizagem da Matemática.

O texto deste trabalho foi desenvolvido com o objetivo de um embasamento teórico clássico sobre a matemática da criptografia trazendo alguns métodos importantes como a Cifra de Cesar, Cifra afim, Cifra de Vigenère, Cifra de Hill e Criptografia RSA.

Ao final fizemos a apresentação de alguns exemplos de algumas poucas porém interessantes atividades para o professor do ensino básico.

REFERÊNCIAS

2850514. *Number of invertible matrices modulo 26*. [S.l.]: https://math.stackexchange.com/users/117438/user2850514, acesso em 26/06/2021. Citado na página 55.

ANTON, H.; RORRES, C. **Álgebra linear com aplicações – 10a. ed.** Porto Alegre: Bookman, 2012. Citado 3 vezes nas páginas 16, 21 e 45.

BEZERRA, D. de J.; MALAGUTTI, P. L. A.; RODRIGUES, V. C. da S. **Aprendendo criptologia de forma divertida**. Goiânia: http://www.mat.ufpb.br/bienalsbm, 2015. Citado na página 64.

BNCC. **Base Nacional Comum Curricular – Ensino Médio**. Brasília: Ministério da Educação, 2020. Citado na página 14.

COUTINHO, S. C. **Criptografia**. Rio de Janeiro: IMPA/OBMEP, 2015. Citado na página 56.

HEFEZ, A. **Aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2016. Citado na página 22.

MALAGUTTI, P. L. A. **Atividades de Contagem a partir da Criptografia**. Rio de Janeiro: IMPA/OBMEP, 2015. Citado na página 64.

MILIES, C. P. **Tópicos de Álgebra Clássica: Um Prelúdio à Álgebra Moderna**. São Paulo: Editora Livraria da Física, 2020. Citado 2 vezes nas páginas 22 e 35.

OLSAVSKY, G. Groups formed from 2×2 matrices over $\mathbb{Z}_p$. **Mathematics Magazine**, v. 63, n. 4, p. 269–272, Oct. 1990. Citado na página 55.

PCN-EM. **Parâmetros Curriculares Nacionais – Ensino Médio**. Brasília: Ministério da Educação, 1998. Citado na página 15.

ROSEN, K. H. **Elementary Number Theory and Its Applications. 3rd. ed.** Reading: Addison-Wesley Publishing Company, 1993. Citado na página 22.

SHOKRANIAN, S. **Criptografia para iniciantes**. 1. ed. Brasília: Editora Universidade de Brasília, 2005. Citado na página 56.

SINGH, S. **The code book: how to make it, break it, hack it, crack it**. 1. ed. New York: Delacorte Press, 2001. Citado 4 vezes nas páginas 35, 37, 39 e 56.

SINGH, S. **O livro dos códigos**. 1. ed. Rio de Janeiro: Record, 2001. Citado 4 vezes nas páginas 35, 39, 40 e 56.

A – FOLHETOS PARA APLICAÇÃO DAS ATIVIDADES DE CRIPTOGRAFIA

Atividade 1. **A Cifra de César**

Júlio César usou uma cifra de substituição simples para enviar mensagens às suas tropas. Ele substituiu cada letra pela letra que estava 3 casas mais adiante no alfabeto, de modo que “A” foi substituído por “D”, “B” por “E” e assim por diante.

Questão 1. Complete a tabela abaixo para mostrar como cada letra é codificada usando este sistema.

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

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

Questão 2. Usando a Cifra de César, codifique o nome de seu país. Seu amigo obteve a mesma mensagem?

Questão 3. Decodifique esta mensagem, que foi codificada usando a cifra de César da tabela criada na **Questão 1**:

R	U	R	P	D	Q	R	D	F	D	W	D	D	P	R	U	H	V	D

G	D	P	D	V	D	P	D	G	D	V	H	U	R	P	D

D	W	D	F	D	R	Q	D	P	R	U	R

Atividade 2. **Cifra afim.**

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

a) Usando a função afim $f(x) = 2x + 3$, codifique a mensagem CRIPTOGRAFADA.

b) Escreva uma mensagem e codifique-a usando a função $f(x) = 3x$.

c) Sabendo que a função cifradora é $f(x) = 2x + 1$, decodifique a mensagem:

$4529475773332945 \quad 57292555295973$

Atividade 3. **A Cifra de Vigenère.**

Esta é uma atividade a ser realizada em grupos de alunos.

Utilizando a tabela abaixo e a palavra chave **CUBO** codifique uma mensagem e depois envie-a a outro grupo, que deverá decifrá-la.

Tabela A.1 – Quadrado de Vigenère

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

Atividade 4. **Tabelas Mágicas.**

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
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

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
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

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
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

i) Esta é uma atividade que pode ser realizada em duplas.

Codifique seu nome usando uma das cifras dadas nas tabelas acima. Peça ao seu amigo para descobrir qual chave você usou.

NOME: _____

Qual das tabelas mágicas foi usada nesta mensagem cifrada?

ii) Esta é uma atividade para ser realizada em equipes de quatro alunos.

Você e seus amigos estão planejando uma festa surpresa. Para garantir que ninguém mais descubra os detalhes, vocês irão codificá-los.

Cada um de vocês preencherá **UM** dos detalhes abaixo (decidam com antecedência quem fará qual parte). Codifique a resposta usando uma das tabelas acima (nem todos precisam usar a mesma tabela). Quando você terminar a codificação, entregue todos os seus papéis para uma outra equipe para ver se eles conseguem descobrir os detalhes da festa.

QUEM: (de quem é a festa surpresa?)

ONDE: (onde você vai dar a festa?)

DIVERSÃO: (que jogo ou atividade você fará para se divertir?)

PRESENTE: (que presente você vai trazer?)