UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS UNIVERSITÁRIO DE ARAGUAÍNA
CURSO DE LICENCIATURA EM MATEMÁTICA

WELLINGTON DE SOUSA MARTÍNS

APLICAÇÃO DA ÁLGEBRA MODERNA NOS FUNDAMENTOS DA CRIPTOGRAFIA- CIFRAS DE CÉSAR E CIFRAS DE HILL

ARAGUAÍNA
2016

WELLINGTON DE SOUSA MARTÍNS

APLICAÇÃO DA ÁLGEBRA MODERNA NOS FUNDAMENTOS DA CRIPTOGRAFIA- CIFRAS DE CÉSAR E CIFRAS DE HILL

Monografia apresentada ao curso de Licenciatura Plena em Matemática da Universidade Federal do Tocantins, como requisito parcial para a obtenção de título de Licenciado em Matemática.
Orientadora: Prof. Msc. Renata Alves da Silva

ARAGUAÍNA
2016

WELLINGTON DE SOUSA MARTNS

APLICAÇÃO DA ÁLGEBRA MODERNA NOS FUNDAMENTOS DA CRIPTOGRAFIA- CIFRAS DE CÉSAR E CIFRAS DE HILL

Monografia apresentada ao curso de Licenciatura Plena em Matemática da Universidade Federal do Tocantins, como requisito parcial para a obtenção de título de Licenciado em Matemática.

Aprovada em _____/_____/_____.

BANCA EXAMINADORA

Prof.ª Msc. Renata Alves Silva (Orientadora)

Prof. Dr. José Carlos Oliveira Jr

Prof.ª Msc. Samara L. Matos

A Deus,
... pelo discernimento e pela paixão pelos números
À minha mãe ...
... por sua garra, pelo apoio, e incentivo e amor.

AGRADECIMENTOS

Agradeço a todos os professores do colegiado de Matemática, em especial ao Dr. Sinval de Oliveira, por sua seriedade e compromisso, ao Msc. Basilides Temistocles Colunche Delgado, à Msc. Yukiko Massago, ao Msc.

Freud Romão por sua atenção e disposição, incentivo e apoio, e pelas melhorias em sua gestão na coordenação do curso.

Minha orientadora, por sua paciência, disposição em me orientar, e Dr. José Carlos Oliveira Jr esclarecimentos e camaradagem.

À Dra. Elisângela Mello e Dr. Jamur André Venturin, Dr. Deive Barbosa Alves por ceder espaço no laboratório da matemática e auxílio.

“A matemática é a rainha das ciências, e a teoria dos números é a rainha da matemática”

Carl Freidrich Gauss (1777-1855).

RESUMO

A comunicação é essencial em toda e qualquer comunidade e, mesmo anteriormente à invenção da escrita, o homem utilizava símbolos para expressar seus sentimentos e cultura. Com a invenção da escrita, que data do século V a. C., veio a possibilidade de difusão da informação. Para manter o sigilo de certas informações, surgiu a criptografia, que veio evoluindo paralelamente aos avanços da tecnologia. Assim, como na antiguidade, os árabes utilizavam uma cifra de substituição monoalfabética para proteger segredos de estado, hoje utilizamos o algoritmo RSA em *Certificados Digitais.* Com a internet, é cada vez maior o número de pessoas que conseguem ter acesso à informação. Hoje, a criptografia é algo comum em nosso dia-a-dia. Os processos de codificação das mensagens enviadas dependem exclusivamente de recursos da matemática, especificamente da álgebra e teoria dos números. Assim, faremos uma introdução ao estudo de criptografia, baseado em sua fundamentação, apresentando alguns dos sistemas que utilizam esses recursos na codificação de suas mensagens, demonstrando os conceitos matemáticos aplicados de forma sucinta e em seguida, apresentaremos uma descrição dos primeiros indícios do surgimento da criptografia na história, como também as contribuições da criptografia para desenvolvimento científico e tecnológico atual.

Palavras-chave: Criptografia. Congruência. Teoria de Grupos.

ABSTRACT

Communication is essential in every community and, even before the invention of writing, man used symbols to express his feelings and culture. With the invention of writing, which dates from the fifth century b. C., came the possibility of diffusion of the information. In order to keep the information secret, cryptography emerged, evolving alongside advances in technology. Thus, as in antiquity, the Arabs used a monoalphabetic substitution cipher to protect state secrets, today we use the RSA algorithm in Digital Certificates. With the internet, more and more people are able to access information. Today, encryption is commonplace in our day-to-day lives. The coding processes of the messages sent depend exclusively on mathematical resources, specifically on algebra and number theory. Thus, we will make an introduction to the study of cryptography, based on its foundation, presenting some of the systems that use these resources in the codification of their messages, demonstrating the mathematical concepts applied succinctly, then a description of the first signs of the emergence of cryptography in history, a well as the contributions of cryptography to current scientific and technological development.

Keywords: Encryption. Congruency. Groups Theory.

SUMÁRIO

INTRODUÇÃO

A criptografia é uma área que vem se desenvolvendo devido à necessidade de se ter uma comunicação por um meio em que apenas o destinatário da mensagem tenha acesso às informações enviadas. Hoje, na era da informação, onde sistemas são invadidos constantemente por hackers, a transferência de dados utilizando um canal seguro é imprescindível para os governos, e a preocupação em manter em segredo informações é algo cotidiano (compras por cartão de crédito via internet, saques em caixas eletrônicos, enviar mensagens via aplicativos, etc, onde podemos (e deve-se) encontrar a criptografia).

A criptografia sempre esteve presente na história do homem, desde a simples transposição de letras para codificação de uma mensagem até a criptografia RSA, hoje um dos sistemas de criptografia mais utilizados no mundo devido à sua segurança.

Conforme afirma Singh em [7]: a Primeira Guerra Mundial é considera a guerra dos químicos devido ao uso do gás mostarda e do cloro; a Segunda Guerra Mundial a dos físicos devido à construção da bomba atômica; e que uma Terceira Guerra Mundial seria a guerra dos matemáticos, porque estes terão o controle sobre a próxima grande arma de guerra: a informação. Buscando compreender esse processo de codificar e decodificar informações, estudamos alguns tipos de criptografias, dando maior ênfase aos primórdios da criptografia moderna: as cifras de substituição e transposição, que, até onde entendemos, são pouco abordadas em outros trabalhos. No primeiro capítulo, fundamentação teórica, abordamos os conceitos de grupos e anéis, especificamente grupos aditivos, multiplicativos, grupo das permutações e o anel $\mathbb{Z}_m$. Em seguida, no segundo capítulo, fazemos uma descrição da origem da criptografia na história. No terceiro capítulo, descrevemos os sistemas criptográficos utilizados em nossa pesquisa, onde os conceitos algébricos são aplicados tanto nos processos criptográficos quanto na verificação de sua segurança.

1. PRELIMINARES

Neste capítulo, apresentaremos conceitos matemáticos básicos que darão suporte para compreendermos o estudo de criptografia. Conceitos de álgebra moderna que são empregados na criptologia, especificamente em mensagens criptografadas em cifras de César e de Hill.

1.1 GRUPOS

Definição 1.1.1: *Seja G um conjunto não vazio onde está definida uma operação entre pares de G, denotada por $* : G \times G \to G$ tal que*

$$(x, y) \longmapsto x * y$$

Dizemos que o par $(G,*)$ é um grupo se são válidas as seguintes propriedades:

G_1) $a * (b * c) = (a * b) * c \; \forall \; a, b, c \in G$.

G_2) $\exists e \in G$ tal que $a * e = e * a, \forall \; a \in G$.

G_3) $\forall \; a \in G, \exists b \in G \; tal$ que $a * b = b * a = e$.

Chamamos a propriedade G_1) de *associatividade*, e o elemento e da propriedade G_2 recebe o nome de identidade do grupo $(G,*)$. É possível mostrar que este elemento é único no conjunto G que satisfaz tal propriedade. Ao elemento b da propriedade $G3$), denominamos inverso de a e denotamos por a^{-1}. Afirmamos que o inverso de a é o único elemento de G que satisfaz a propriedade $G3$). De fato, se $a * b_1 = b_1 * a = e$ e $a * b_2 = b_2 * a = e$, segue que $b_1 = e * b_1 = (b_2 * a) * b_1 = b_2 * (a * b_1) = b_2 * e = b_2$. Ou seja, o inverso de a é único, como havíamos afirmado. Se em um grupo $(G,*)$, verifica-se a propriedade de comutatividade:

G_4) $a * b = b * a, \forall \; a, b \in G$, dizemos que o grupo $(G,*)$ é um *grupo abeliano* (em honra ao matemático Norueguês N. H. Abel – 1802-1829).

Usaremos a notação G em vez de $(G,*)$ para denotar um grupo. Também usaremos ab ao invés de $a * b$, para representarmos o resultado de a operado com b. A operação de G será sempre explicitada no contexto, e usaremos a notação aditiva $a * b = a + b$ apenas para grupos abelianos e, nesse caso, a identidade será representada por 0.

Definição 1.1.2: *A ordem de um grupo G, denotada por $|G|$, é o número de elementos de G. Dizemos que a sua ordem é infinita quando G é um grupo infinito, e denotamos por $|G| = +\infty$.*

(i) Grupos aditivos.

Os conjuntos $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ e $(\mathbb{C}, +)$ são exemplos de grupos aditivos. São grupos de ordem infinita. Essa afirmação segue das propriedades da operação de adição definidas sobre esses conjuntos.

(ii) Grupos lineares de grau n (multiplicativo, não comutativo se $n > 1$).

Indicaremos por K, indistintamente um dos conjuntos $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ e por $M_n(K)$ o conjunto das matrizes de ordem n sobre K. Uma vez que a soma de matrizes em $M_n(K)$ herda propriedades de grupo do conjunto K, não é difícil ver que $M_n(K)$ é um grupo aditivo abeliano. No que se refere à multiplicação de matrizes, a situação é diferente.

Para multiplicação de matrizes, vale a associatividade e, além disso, ela conta com elemento neutro que é a matriz identidade de ordem n,

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Embora satisfaça as propriedades $G1)$ e $G2)$, este conjunto, munido da operação de multiplicação, não satisfaz a propriedade $G3)$, uma vez que a matriz nula, dada por

$$O_n = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

multiplicada por uma matriz qualquer é ela mesma, portanto, diferente de I_n.

Para saber quais as matrizes de ordem n têm inversa, recorremos ao seguinte teorema da teoria dos determinantes: Uma matriz $A \in M_n(K)$ é inversível se, e somente se, $detA \neq 0$.

Como o conjunto das matrizes inversíveis, que indicaremos por $GL_n(K)$, inclui a matriz identidade I_n, cujo determinante é igual a 1 e $det(AB) = (detA)(detB) \neq 0$, $\forall\, A, B \in GL_n(K)$, então $(GL_n(K), \cdot)$ é um grupo, onde a operação $\cdot$, é a multiplicação de matrizes. Esse grupo não é comutativo quando $n > 1$, pois, por exemplo, se

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \text{ e } B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix},$$

então

$$AB = \begin{pmatrix} n & \cdots & 1 \\ \vdots & \cdots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} \neq BA = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \cdots & \vdots \\ 1 & \cdots & n \end{pmatrix}.$$

O grupo $(GL_n(K), \cdot)$ é chamado grupo linear racional (quando $K = \mathbb{Q}$), grupo linear real (quando $K = \mathbb{R}$), grupo linear complexo (quando $K = \mathbb{C}$), de grau n.

(iii) Grupos aditivos de classes de restos (comutativos).

Neste exemplo, considere um inteiro $m > 1$. Vamos definir uma relação de equivalência sobre o conjunto $\mathbb{Z}$ da seguinte maneira: x é equivalente a y se, e somente se, os restos da divisão de x e y por m são iguais. É possível mostrar que esta relação define, de fato, uma relação de equivalência. Vamos denotar por $\bar{x}$ o conjunto de todos os inteiros y que são equivalentes a x. Como os possíveis restos da divisão de um número inteiro qualquer por m pertence ao conjunto $\{0,1,\ldots,m-1\}$, segue que $\mathbb{Z}$ é a união disjunta $\bar{0} \cup \bar{1} \cup \ldots \cup \overline{\{m-1\}}$. Definimos $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. Neste conjunto, a adição é definida da seguinte maneira:

$$\bar{a} + \bar{b} := \overline{a+b}$$

e é uma operação sobre $\mathbb{Z}_m$ para a qual vale a associatividade e comutatividade. Além disso,

$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a} \; \forall \; a \in \mathbb{Z}$$

e, portanto, $\bar{0}$ é o elemento neutro dessa operação. A classe $\overline{m-a}$ é o oposto de $\bar{a} \in \mathbb{Z}_m$ na adição, pois

$$\bar{a} + \overline{m-a} = \overline{a+(m-a)} = \bar{m} = \bar{0},$$

uma vez que, na divisão de m por m, o resto é 0. Então,

$$-\bar{a} = \overline{m-a}.$$

Após essas considerações, $(\mathbb{Z}_m, +)$ é um grupo comutativo, para todo inteiro $m > 1$, chamado grupo aditivo das classes de resto módulo m. Vale notar que a ordem desse grupo é m.

(iv) Grupos multiplicativos de classes de restos.

A multiplicação em $\mathbb{Z}_m$ é definida da seguinte maneira: para $\bar{a}, \bar{b} \in \mathbb{Z}_m$, definimos $\bar{a} \cdot \bar{b} = \overline{ab}$. Esta operação está bem definida e goza das propriedades associativa e comutativa. Além disso, a classe $\bar{1}$, é o elemento neutro, uma vez que $\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a}$ para todo $a \in \mathbb{Z}$.

Mas, excluindo-se o elemento $\bar{0}$ em $\mathbb{Z}_m$, que não possui inverso para a multiplicação, nem sempre o conjunto restante é um grupo. De fato, a operação de multiplicação restrita ao conjunto $\mathbb{Z}_4 \setminus \{0\}$, por exemplo, sequer está bem definida, uma vez que $\bar{2} \cdot \bar{2} = \overline{2 \cdot 2} = \bar{4} = \bar{0} \notin \mathbb{Z}_4 \setminus \{0\}$.

Provaremos agora o seguinte resultado sobre o conjunto $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$.

Lema 1.1.1: *A operação de multiplicação é uma operação em $\mathbb{Z}_m^*$ se, e somente se, m é primo.*

Demonstração: Suponhamos que m não seja primo. Como $m > 1$, podem ser encontrados dois inteiros $a, b > 1$ tais que $ab = m$.

Dessa igualdade, resulta que $\bar{a} \cdot \bar{b} = \overline{ab} = \bar{m} = \bar{0}$ então $\bar{a} \cdot \bar{b} = \bar{0} \notin \mathbb{Z}_m^* \backslash \{0\}$, que é impossível em face da hipótese. Reciprocamente, a única possibilidade de a multiplicação módulo m, quando restrita aos elementos de $\mathbb{Z}_m^*$, não ser uma operação sobre esse conjunto é acontecer de $\bar{a} \cdot \bar{b} = \bar{0}$ para algum par de elementos desse conjunto. Mas isso implicaria $\bar{a} \cdot \bar{b} = \bar{0}$ e, portanto, ab deixa resto 0 na divisão por m, isto é, ab é um múltiplo de m. Como m é primo por hipótese, então m divide a ou m divide b. Considerando-se, sem perda de generalidade, o caso $a = mq$, para algum inteiro q, temos

$$\bar{a} = \overline{mq} = \bar{m} \cdot \bar{q} = \bar{0} \cdot \bar{q} = \overline{0 \cdot q} = \bar{0},$$

o que é um absurdo, visto que, por hipótese $\bar{a} \in \mathbb{Z}_m^*$. □

Mostraremos agora que, se m é primo, a multiplicação módulo m, quando restrita aos elementos de $\mathbb{Z}_m^*$ faz desse conjunto um grupo. Para isto basta mostrar que, qualquer que seja o elemento $\bar{a} \in \mathbb{Z}_m^*$, pode-se encontrar $\bar{b} \in \mathbb{Z}_m^*$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$. De fato, como $\bar{a} \in \mathbb{Z}_m^*$, então $\text{mdc}(m, a) = 1$. Daí, $mx_0 + ay_0 = 1$, para convenientes inteiros x_0 e y_0 (este resultado é conhecido como Identidade de Bezout; veja [2]). Assim,

$$\bar{1} = \overline{mx_0 + ay_0} = \bar{m} \cdot \overline{x_0} + \bar{a} \cdot \overline{y_0} = \bar{a} \cdot \overline{y_0},$$

o que mostra que $\overline{y_0}$ (que pertence a $\mathbb{Z}_m^*$) é o inverso de $\bar{a}$.

As considerações anteriores permitem concluir que $\mathbb{Z}_m^*$ é um grupo multiplicativo se, e somente se, m é primo.

Vamos fazer um exemplo mais palpável. Determinemos o inverso de $\bar{4}$ em $\mathbb{Z}_5^*$, usando o raciocínio da última demonstração. Ora, uma solução de $5x_0 + 4y_0 = 1$, que pode ser determinada por simples observação, é $(1, -1)$. Logo, $y_0 = -1$ e, portanto, o inverso de $\bar{4}$ é $\overline{-1} = \bar{4}$.

(iv) Grupos das Permutações.

Permutação é o termo específico usado na teoria dos grupos para designar uma bijeção de um conjunto nele mesmo. Se E indica um conjunto não vazio, denotaremos por $S(E)$ conjunto das permutações dos elementos de E. A composição, nesse caso, é uma operação sobre $S(E)$, pois, se f e g são permutações de E, ou seja, se $f: E \to E$ e $g: E \to E$ são bijeções, então a composta, $g \circ f: E \to E$, também é uma bijeção. A associatividade é válida para essa operação e, se $i_E: E \to E$ for a aplicação identidade, que claramente é uma bijeção,

temos que i_E é o elemento neutro de $S(E)$, posto que: $(i_E \circ f)(x) = i_E\big(f(x)\big) = f(x)$, para todo $x \in E$, o que garante a igualdade $i_E \circ f = f$, $\forall\, f \in S(E)$. Finalmente, se f é uma permutação de E, então o mesmo acontece com f^{-1}(aplicação inversa de f), que é uma bijeção e é o elemento inverso de f para a composição de aplicações, pois $f \circ f^{-1} = f^{-1} \circ f = i_E$.

Portanto, $(S(E),\circ)$ é um grupo chamado de *grupo das permutações sobre E*. Esse grupo é comutativo se, e somente se, sua ordem é 1 ou 2. De fato, se a ordem é 1, $S(E)$ só possui um elemento, a aplicação identidade que, naturalmente, comuta consigo mesma. Se a ordem é 2 e os elementos de E forem indicados por a e b, então $S(E)$ também só tem dois elementos: a aplicação identidade e a aplicação que leva a em b, e vice-versa. Como, obviamente, a última aplicação comuta consigo mesma e com i_E, então $(S(E),\circ)$ também é comutativo nesse caso.

Suponhamos agora que o $|S(E)| > 2$ e que, portanto, E tenha mais do que 2 elementos. Designando por a, b e c três elementos distintos de E, consideremos as permutações f e g de $S(E)$ definidas da seguinte maneira:

$$f(a) = b, f(b) = a \quad \text{e} \quad f(x) = x \text{ qualquer que seja } x \neq a, b$$

e

$$g(a) = c, g(c) = a \quad \text{e} \quad g(x) = x \text{ qualquer que seja } x \neq a, c.$$

É claro que f e g são permutações de E, pela maneira como foram construídas. Além disso,

$$(f \circ g)(a) = f\big(g(a)\big) = f(c) = c$$

e

$$(g \circ f)(a) = g\big(f(a)\big) = g(c) = a,$$

o que mostra que $g \circ f \neq f \circ g$ e, portanto, que $S(E)$ não é comutativo.

Muitas vezes, para simplificar cálculos e notações, para $f \in S_k$(ao invés de usarmos a notação genérica $S(E)$, usamos S_k, para representar o conjunto das permutações sobre E chamado de *grupo simétrico de grau n*) $f(1) = i_1, f(2) = i_2, \ldots, f(k) = i_k$, escrevemos

$$f = \begin{pmatrix} 1 & 2 & \cdots & k \\ i_1 & i_2 & \cdots & i_k \end{pmatrix}.$$

Por exemplo a permutação identidade é denotada por

$$\begin{pmatrix} 1 & 2 & \cdots & k \\ 1 & 2 & \cdots & k \end{pmatrix}.$$

Uma observação importante que pode ser feita é que a ordem das colunas não importa, embora, em geral, se usem os elementos da primeira linha em ordem crescente. Por exemplo, em S_3,

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}=\begin{pmatrix}2 & 3 & 1\\ 1 & 3 & 2\end{pmatrix},$$

pois ambas têm o mesmo efeito sobre os elementos de E.

Definimos a composição de duas permutações

$$f=\begin{pmatrix}1 & 2 & \cdots & k\\ i_1 & i_2 & \cdots & i_k\end{pmatrix} \text{ e } g=\begin{pmatrix}1 & 2 & \cdots & k\\ j_1 & j_2 & \cdots & j_k\end{pmatrix}$$

da seguinte maneira:

$$g\circ f=\begin{pmatrix}1 & \cdots & i_r & \cdots & k\\ j_1 & \cdots & j_{i_r} & \cdots & j_k\end{pmatrix}\circ\begin{pmatrix}1 & \cdots & r & \cdots & k\\ i_1 & \cdots & i_r & \cdots & i_k\end{pmatrix}=\begin{pmatrix}1 & \cdots & r & \cdots & k\\ j_{i_1} & \cdots & j_{i_r} & \cdots & j\end{pmatrix},$$

pois $(g\circ f)(r)=g\big(f(r)\big)=g(i_r)=j_{i_r}$.

Definição 1.1.3 *A ordem de um elemento a em um grupo G, denotada por $|a|$, é o menor inteiro positivo n tal que $a^n \coloneqq a\cdot a\dots a=e$. Caso esse inteiro não exista, dizemos que a possui ordem infinita.*

Definição 1.1.4 *Um subconjunto H de um grupo G é **subgrupo G** se H também for um grupo com a operação de G.*

A seguir, daremos alguns exemplos simples de subgrupos, para fixar ideias.

Exemplos 1.1.1

O subconjunto $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\}$ é um subgrupo aditivo de $\mathbb{Z}_{12}$, pois satisfaz as propriedades que definem um grupo (deixamos a demonstração desta afirmação a cargo do leitor). Um outro exemplo, agora em S_4, é o subgrupo D_4, dado por

$$D_4=\left\{\begin{pmatrix}1234\\1234\end{pmatrix},\begin{pmatrix}1234\\2341\end{pmatrix},\begin{pmatrix}1234\\3412\end{pmatrix},\begin{pmatrix}1234\\4123\end{pmatrix},\begin{pmatrix}1234\\4321\end{pmatrix},\begin{pmatrix}1234\\2143\end{pmatrix},\begin{pmatrix}1234\\1432\end{pmatrix},\begin{pmatrix}1234\\3214\end{pmatrix}\right\}.$$

É possível mostrar que D_4 é um subgrupo de S_4, cuja ordem é 8.

1.2 ANÉIS

Apresentaremos nesta seção conceitos de estruturas algébricas fundamentais utilizados na criptografia de César e Hill. Basicamente, veremos os conceitos de ideais, anel quociente, o anel $\mathbb{Z}_m$e o anel $M_m(\mathbb{Z}_m)$.

Definição 1.2.1: Seja A um conjunto não vazio onde estejam definidas duas operações, as quais chamaremos de *soma* e *produto* em A e denotaremos (como em $\mathbb{Z}$) por $+$ e $\cdot$ definidas como

$$+:A\times A\to A \qquad \text{e} \qquad \cdot:\ A\times A\to A$$
$$(a,b)\longmapsto a+b \qquad\qquad (a,b)\longmapsto a\cdot b$$

que satisfazem:

(i) (A, +) é um grupo abeliano.

(ii) O produto é distributivo em relação à adição, isto é, se $a, b, c \in A$, então $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$. Se assim for, chamamos o termo (A, +, ·) de um *Anel*.

Por uma questão de simplicidade de linguagem, poderemos identificar a adição do anel com símbolo + e a multiplicação com um ponto. E quando não houver possibilidade de confusão, até os símbolos poderão ser omitidos. Por exemplo, será comum usarmos as expressões como "Seja (A,+, ·) um anel" ou mesmo" Seja A um anel" ou" Consideramos um anel". Naturalmente, as duas últimas alternativas pressupõem que não haja confusão possível quanto às operações subentendidas. Outra maneira simplificada de nos referirmos a um anel A será dizendo que *"A* tem uma estrutura de anel", o que naturalmente também pressupõe as operações já subentendidas.

Seja (A,+, ·) um anel. As propriedades aqui reunidas são conseqüências do fato de que a adição é uma operação sobre A e de que (A, +) é um grupo aditivo abeliano.

- O elemento neutro 0_A é único. Esse elemento é chamado de *zero* do anel e poderá ser indicado apenas por 0.
- O oposto $-a$ de um elemento A do anel é único.
- Se $a_1, a_2, \dots, a_n \in A$, então $-(a_1 + a_2 + \cdots + a_n) = (-a_1) + (-a_2) + \cdots + (-a_n)$. (Observar que a comutatividade da adição foi usada.)
- Se $a \in A$, então $-(-a) = a$.
- Se $a + x = a + y$, então $x = y$. Ou seja, todo elemento de A é regular para a adição. ou dito, em outros termos, vale a *lei do cancelamento da adição.*
- A equação $a + x = b$ tem uma só solução: o elemento $b + (-a)$.

(a) Se $a \in A$, então $a \cdot 0 = 0 \cdot a = 0$.

Demonstração:

$$\underline{0 + a \cdot 0} = a \cdot 0 = a \cdot (0 + 0) = \underline{a \cdot 0 + a \cdot 0}$$

(cancelando $a \cdot 0$)

$$\downarrow$$

$$0 = a \cdot 0$$

Analogamente, se demonstra que $0 \cdot a = 0$.

(b) Se $a, b \in A$, então $a(-b) = (-a)b = -(ab)$.

Demonstração:

$$\underbrace{ab + [-(ab)]} = 0 = a \cdot 0 = a[b + (-b)] = \underbrace{ab + a(-b)}$$

(cancelando ab)

$$-(ab) = a(-b).$$

Analogamente, se demonstra que $-(ab) = (-a)b$.

(c) Se $a, b \in A$, então $(-a)(-b) = ab$.

Demonstração: Devido à propriedade anterior, $(-a)(-b) = -[a(-b)]$. Pelo mesmo motivo, $a(-b) = -(ab)$. Portanto,

$$(-a)(-b) = -a[(-b)] = -[-(ab)] = ab.$$

Definição 1.2.2 (*diferença* em um anel): Sejam $a, b \in A$. Chama-se *diferença* entre a e b e indica-se por $a - b$ o elemento $a + (-b) \in A$. Portanto, $a - b = a + (-b)$.

(a) Se $a, b \in A$, então $a(b - c) = ab + (-ac) = ab - ac$.

Demonstração: Temos que $a(b - c) = a[b + (-c)] = ab + a(-c)$. Como, porém, $a(-c) = -ac$, tem-se:

$$a(b - c) = ab + (-ac) = ab - ac.$$

Deixamos como exercício a demonstração de que $(a - b)c = ac - bc$.

Se a multiplicação de A goza da propriedade comutativa, isto é, se $ab = ba$, para quaisquer $a, b \in A$, então se diz que A é um *anel comutativo.*

Exemplos 1.2.1

Um bom e simples exercício é mostrar que $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são anéis com as operações conhecidas definidas. Além disso, são anéis comutativos.

Exemplos 1.2.2

Os anéis $\mathbb{Z}_m$ das classes de resto são anéis. De fato, se a, $b \in \mathbb{Z}_m$,então $\bar{a} \cdot \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \cdot \bar{a}$, pois o resto da divisão de ab por m é igual ao resto da divisão de ba por m.

O terno $(M(A), +, \cdot)$ é um exemplo de anel chamado Anel das matrizes de ordem n.

Não são comutativos os anéis $M_n(K)$, em que K indica $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ se $n > 1$. De fato, se $n > 1$ e

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Então, $AB \neq BA$, como já foi verificado anteriormente.

1.2.1 - Subanéis

Definição 1.2.5 Sejam $(A, +, \cdot)$ um anel e L um subconjunto não vazio de A. Diz-se que L é subanel de A se as seguintes condições forem satisfeitas:

(i) L é fechado, isto é, se $a, b \in L$, então $a + b \in L$ e $a \cdot b \in L$. Para as operações que fazem o conjunto A ter a estrutura de anel;

(ii) $(L, +, \cdot)$ também é um anel. (Naturalmente, a adição e multiplicação consideradas são as mesmas de A, porém, restritas aos elementos de L).

Exemplos 1.2.2

- Considerando-se as operações usuais sobre os conjuntos numéricos: $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{Q}$ é um subanel de $\mathbb{R}$ e $\mathbb{C}$;$\mathbb{R}$ é um subanel de $\mathbb{C}$.
- $M_n(\mathbb{Z})$ é um subanel de $M_n(\mathbb{Q}), M_n(\mathbb{R})$ e $M_n(\mathbb{C})$; $M_n(\mathbb{Q})$ é subanel de $M_n(\mathbb{R})$ e $M_n(\mathbb{C})$; $M_n(\mathbb{R})$ é subanel de $M_n(\mathbb{C})$.

1.2.2 Ideais

Definição 1.2.6 - Seja A um anel e seja I um subanel de A. Dizemos que I é um *ideal à esquerda* de A se

(i) $a \cdot x \in I, \ \forall\, a \in A, \ \forall\, x \in I$ (ou simbolicamente $A \cdot I \subset I$).

Analogamente, definimos um ideal à direita J de um anel A como sendo um subanel de A satisfazendo a condição

(i)' $x \cdot a \in J, \ \forall\, a \in A, \forall\, x \in J$ (ou simbolicamente $A \cdot J \subset J$).

Se I é um ideal simultaneamente à direita e à esquerda de um anel A dizemos que I é *ideal* de A, isto é, I é um ideal de A se

(ii) $A \cdot I \subset I$ e $I \cdot A \subset I$.

* Se o anel A for comutativo, então as condições (i), (i)' e (ii) são equivalentes, e as 3 noções acima coincidem.

Claramente $\{0\}$ e A são ideais de A (ditos *ideais triviais* de A). Os ideais não triviais de A são chamados *ideais próprios* de A.

Exemplo 1.2.3 Seja A o anel $M_2(\mathbb{R}) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}\right\}$ e sejam I e J subconjuntos de A definidos por

$$I = \left\{\begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} : a, c \in \mathbb{R}\right\} \text{ e } J = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R}\right\}.$$

Pode-se mostrar que I é um ideal à esquerda de A e J é um ideal à direita de A, mas nenhum dos dois é ideal de A. Aliás, vamos provar agora que os únicos ideais de $A = M_2(\mathbb{R})$ são triviais (por isso, A é chamado de *um anel simples*). De fato, seja P um ideal de $A =$

$M_2(\mathbb{R})$ e vamos assumir que $P \neq \{0\}$. Assim $\exists \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in P$ tal que algum dos $a_{ij}'s$ é diferente de zero, $1 \leq i, j \leq 2$. Sejam $e_{rs} \in M_2(\mathbb{R})$, $1 \leq r, s \leq 2$, as seguintes matrizes:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$e_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, e_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, e_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \text{ e } e_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Através de cálculos, pode se verificar que $e_{rs} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{mn}$ é uma matriz 2×2 contendo o elemento a_{sm} na posição (r, n) da matriz. Logo, como $A \cdot P \subset P$ e $P \cdot A \subset I$, segue que

$e_{1s} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{m1} = \begin{bmatrix} a_{sm} & 0 \\ 0 & 0 \end{bmatrix} \in I$, onde$1 \leq s, m \leq 2$, e também

$e_{2s} \cdot \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot e_{m2} = \begin{bmatrix} 0 & 0 \\ 0 & a_{sm} \end{bmatrix} \in I$ onde$1 \leq s, m \leq 2$.

Daí, concluímos que, se $1 \leq s, m \leq 2$, temos

$$\begin{bmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{bmatrix} = \begin{bmatrix} a_{sm} & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & a_{sm} \end{bmatrix} \in P.$$

Escolhemos s, m de modo que $a_{sm} \neq 0$. Dessa forma,

$\begin{bmatrix} {a_{sm}}^{-1} & 0 \\ 0 & {a_{sm}}^{-1} \end{bmatrix} \cdot \begin{bmatrix} a_{sm} & 0 \\ 0 & a_{sm} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in P$, e como $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ é unidade do anel A,

segue imediatamente que $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in P$ quaisquer que sejam $a, b, c, d \in \mathbb{R}$, isto é, $P = M_2(\mathbb{R})$, como queríamos demonstrar.

A seguir, apresentaremos uma definição de ideal para um anel comutativo.

Definição 1.2.7 Seja A um anel comutativo. Um conjunto $I \subset A$, $I \neq \emptyset$, será chamado de **ideal** em A se, para quaisquer $x, y \in I$ e para qualquer $a \in A$, verificarem-se as relações seguintes: (i) $x - y \in I$; (ii) $ax \in I$.

Exemplo 1.2.4 Se A indica um anel comutativo, então $\{0_A\}$ e o próprio A são ideais em A. São chamados de *ideais triviais* do anel.

Exemplo 1.2.5 Considere em $\mathbb{Z}$ os subconjuntos $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ qualquer que seja o inteiro n. Neste caso, $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$. De fato,

- se $x, y \in n\mathbb{Z}$, então $x = rn$ e $y = sn$ para convenientes inteiros r e s. Logo, $x - y = rn - sn = (r - s)n$, em que $r - s$ é inteiro. De onde $x - y$ $n\mathbb{Z}$.
- seja $a \in \mathbb{Z}$ e $x \in n\mathbb{Z}$. Então, $x = nq$ $(q \in \mathbb{Z})$ e, portanto, $ax = a(nq) = (aq)n$, em que aq é inteiro, o que mostra que $ax \in n\mathbb{Z}$.

1.2.3 Anéis Quocientes

Veremos agora que a definição de ideal nos permite generalizar a noção de congruência módulo m em $\mathbb{Z}$. Considere $J = n \cdot \mathbb{Z}$ e $x, x' \in \mathbb{Z}$, onde n é um inteiro qualquer. Então, $x \equiv x' (\mathrm{mod}\, m) \Leftrightarrow x - x' \in J$ (é também usual escrever $x \equiv x' (\mathrm{mod}\, J)$) define uma relação de equivalência em $\mathbb{Z}$. Agora, vamos generalizar essa idéia para um anel qualquer.

Definição 1.2.8: Seja A um anel qualquer e seja J um ideal de A. Vamos definir a seguinte relação em A:

$$\text{se } x, x' \in A,\ x \equiv x' (\mathrm{mod}\, J) \Leftrightarrow x - x' \in J.$$

Mas, primeiramente, vamos provar que a relação definida acima é, de fato, uma relação de equivalência. Para isso, quaisquer que sejam $x, x', x'' \in A$, temos

(i) $x \equiv x\ (\mathrm{mod}\, J)$, pois $0 = x - x \in J$.

(ii) $x \equiv x' (\mathrm{mod}\, J) \Rightarrow x' \equiv x (\mathrm{mod}\, J)$, pois , se $x - x' \in J$, então $x' - x = -(x - x') \in J$.

(iii) $x \equiv x' (\mathrm{mod}\, J)$ e $x' \equiv x'' (\mathrm{mod}\, J) \Rightarrow x \equiv x'' (\mathrm{mod}\, J)$, pois $x - x' \in J$ e $x' - x'' \in J \Rightarrow x - x'' = (x - x') + (x' - x'') \in J$.

Denotaremos por $\bar{x} = \{y \in A : y \equiv x (\mathrm{mod}\, J)\}$ e chamaremos de *classe de equivalência* do elemento $x \in A$ relativamente à relação $\equiv (\mathrm{mod}\, J)$.

Agora, observe que $y \in \bar{x} \Leftrightarrow y - x \in J$ e, por isso, também denotaremos a classe $\bar{x}$ por $\bar{x} = x + J = \{x + z : z \in J\}$. Chamaremos de *conjunto quociente de A pelo ideal J* ao conjunto $A/J = \{\bar{x} = x + J : x \in A\}$. Tomando $J = m$, definimos a relação de congruência módulo m.

Vamos provar agora uma proposição que nos permitirá definir as operações + e $\cdot$ no conjunto quociente A/J de modo a torná-lo um anel.

Proposição 1.2.1. *Sejam A um anel e J um ideal de A. Se* $x \equiv x' (\mathrm{mod}\, J)$ *e* $y \equiv y' (\mathrm{mod}\, J)$, então: (a) $x + y \equiv (x' + y') (\mathrm{mod}\, J)$

(b) $x \cdot y \equiv x' \cdot y' (\mathrm{mod}\, J)$.

Demonstração: (a) Basta observar que $(x + y) - (x' + y') = (x - x') + (y - y') \in J$.

(b) Agora, sejam $x = x' + a, a \in J$, e $y = y' + b, b \in J$. Então,

$$x \cdot y - x' \cdot y' = (x' + a) \cdot (y' + b) - x' \cdot y' = x' \cdot b + a \cdot y' + a \cdot b = x' \cdot b + a \cdot y' ab$$

e, como a, b pertence m a A e J é um *ideal* de A, segue que $x \cdot y - x' \cdot y' \in J$, como queríamos demonstrar.

Proposição 1.2.3. *Sejam A um anel e J um ideal de A.* Se $\bar{x} = \bar{x}'$ e $\bar{y} = \bar{y}'$, então

(a) $\overline{x + y} = \overline{x' + y'}$.

(b) $\overline{x \cdot y} = \overline{x' \cdot y'}$.

O item (a) diz que a classe da soma independe dos representantes das classes das parcelas, enquanto o item (b) diz que a classe do produto independe dos representantes das classes dos fatores. Isso mostra que tanto a soma quanto o produto estão bem definidos no Anel quociente A/J. Deixamos esta demonstração como exercício para o leitor. O próximo resultado complementa esta observação.

Teorema 1.2.1. *Sejam A um anel e J um ideal de A. Se* $\bar{x} = x + J$ e $A/J = \{\bar{x}: x \in A\}$, *então*

(a) $+ : A/J \times A/J \to A/J$ e $\cdot : A/J \times A/J \to A/J$

$(\bar{x}, \bar{y}) \longmapsto \bar{x} + \bar{y} = \overline{x + y}$ $(\bar{x}, \bar{y}) \longmapsto \bar{x} \cdot \bar{y} = \overline{x \cdot y}$

definem duas operações (denominaremos soma e produto)em A/J.

(b) $(A/J, +, \cdot)$ *é um anel (chamado* anel quociente de *A* por *J*).

(c) *Se* 1 *é a unidade de A, então* $\bar{1}$ *é a unidade de* A/J.

(d) *Se A é comutativo, então* A/J *é comutativo.*

Demonstração: (a) Pela Proposição 1.2.3, as regras

$$\bar{x} + \bar{y} = \overline{x + y} \quad \text{e} \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

são operações bem definidas no conjunto A/J.

(b) Não é difícil ver que tais operações fazem do terno $(A/J, +, .)$ um Anel.

(c) $1 \cdot x = x \cdot 1 = x \; \forall \in A \Rightarrow \bar{1} \cdot \bar{x} = \bar{x} \cdot \bar{1} = \bar{x}, \; \forall \, \bar{x} \in A/J$. Isso mostra que $\bar{1}$ é a unidade do Anel A/J.

(d) Se $x \cdot y = y \cdot x \;\; \forall \, x, y \; \in A$, então claramente, temos,

$$\bar{x} \cdot \bar{y} = \bar{y} \cdot \bar{x} \quad \forall \, \bar{x}, \bar{y} \; \in A/J.$$

Isso mostra que, de fato, A/J é comutativo se A o for.

Exemplo 1.2.6: O anel $\mathbb{Z}_n$

Se $J = n \cdot \mathbb{Z}$, para algum número inteiro n, a relação $\equiv (\mathrm{mod}\, m)$ pode também ser definida por

$$x, x', x'' \in \mathbb{Z}, \; x \equiv x' (\mathrm{mod}\, m) \Leftrightarrow x - x' \in J \Leftrightarrow x \; \equiv \; x' \, \mathrm{mod}\, J.$$

Usaremos a notação $\bar{x} = x + J = \{x + kn : k \in \mathbb{Z}\}$ para classes de equivalência de x em relação a $\equiv (\mathrm{mod}\, m)$. Usaremos também a notação $\mathbb{Z}_n$, $\mathbb{Z}/J$ ou $\mathbb{Z}/_{n \cdot \mathbb{Z}}$ para simbolizar o conjunto quociente de $\mathbb{Z}$ módulo J. E, pelo Teorema 1.2.1, $\mathbb{Z}_n$ é um *anel comutativo com unidade* $\bar{1}$.

1.2.4 Domínio ou Anéis de Integridade

Nesta seção, definiremos o conceito de Domínio ou Anel de Integridade. Este conceito é o mais próximo da ideia de Corpo na Álgebra Moderna.

Definição 1.2.9 Seja A um anel. Se A possui um elemento neutro para a multiplicação, isto é , se existe um elemento $1_A \in A$, $1_A \neq 0$, tal que

$$a \cdot 1_A = 1_A \cdot a = a$$

Para todo $a \in A$, então se diz que 1_A é a *unidade* de A e que A é um *anel com unidade.* Quando não houver possibilidade de confusão, poderemos indicar apenas por 1.

Exemplo 1.2.7

- Os anéis $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$ e $\mathbb{C}$ são anéis com unidade, cuja a unidade é 1.
- Os anéis $\mathbb{Z}_m$ das classes de resto são anéis com unidade. A unidade é a classe $\bar{1}$, pois $\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a}$ e $\mathbb{Z}_m$ é comutativo.
- Os anéis $M_m(K)$, em que K é um dos anéis $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$ ou $\mathbb{C}$, também é um exemplo de anel com unidade. A unidade é a matriz

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Definição 1.2.10 Seja A um anel comutativo com unidade. Se para esse anel vale a lei do anulamento do produto, ou seja, uma igualdade do tipo

$$ab = 0_A,$$

em que $a, b \in A$, implicar

$$a = 0_A \text{ ou } b = 0_A,$$

então se diz que A é um *anel de integridade* ou A é um *domínio*. A forma contrapositiva dessa condição é a seguinte: se $a \neq 0$ e $b \neq 0$, então $ab = 0$.

Exemplo 1.2.8 Todos os anéis $\mathbb{Z}$,$\mathbb{Q}$,$\mathbb{R}$ e $\mathbb{C}$, são anéis de integridade.

Consideremos o anel comutativo A em que não se verifica a lei do anulamento do produto. Isso significa que há pelo menos um par de elementos $a, b \neq 0$ (eventualmente esses elementos são iguais) tais que $ab = 0_A$. Quando isso se verifica, diz-se que a e b *são divisores de zero* do anel. Portanto, um anel de integridade pode ser definido como um anel comutativo com unidade que não possui divisores do próprio zero. Ou, ainda, como um anel

comutativo com unidade cujo conjunto dos elementos diferentes do zero é fechado para a multiplicação.

Exemplo 1.2.9 Se $m > 1$ é um inteiro composto, então sempre há divisores próprios do zero do anel $\mathbb{Z}_m$. De fato, nesse caso, existem inteiros positivos a e b tais que $a, b < m$ e $m = ab$. Portanto, $\bar{a}, \bar{b} \neq 0$ e $\bar{a} \cdot \bar{b} = \overline{ab} = \bar{m} = \bar{0}$. No anel $\mathbb{Z}_4$, por exemplo, o único divisor próprio do zero é o $\bar{2}$ (observe que $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$).

Proposição 1.2.3 Um elemento $\bar{a} \in \mathbb{Z}_m$ é invertível se, e somente se, $mdc\,(a, m) = 1$.

Demonstração**:** Se $\bar{a}$ é invertível, então existe $\bar{b} \in \mathbb{Z}_m$ tal que $\bar{1} = \bar{a} \cdot \bar{b} = \overline{ab}$, isto é, existe um número t tal que $a \cdot b + m \cdot \mathrm{t} = 1$. Assim, se $mdc\,(a, m) = d$, escrevendo $a = dq_1$ e $m = dq_2$, temos que

$$1 = ab + mt = d(q_1 b + q_2 t),$$

o que mostra que $d = 1$. Reciprocamente, se mdc (a,m)=1, pela Identidade de Bézout existem inteiros b e t tais que $a \cdot b + m \cdot \mathrm{t} = 1$ e consequentemente, $\bar{1} = \overline{a \cdot b + m \cdot \mathrm{t}} = \overline{a \cdot b} + \overline{m \cdot t} = \bar{a} \cdot \bar{b} + \bar{0} = \bar{a} \cdot \bar{b}$. Portanto, $\bar{a}$ é invertível.

Proposição 1.2.4 Um anel de classes de restos $\mathbb{Z}_m$ é anel de integridade se, e somente se, m é um número primo.

Demonstração: Se m fosse composto, então $\mathbb{Z}_m$ possuiria divisores próprios do zero, como já se mostrou no exemplo anterior. Mas isso contraria a hipótese. Reciprocamente, como já sabemos $\mathbb{Z}_m$ é um anel comutativo com unidade, qualquer que seja $m > 1$. Suponhamos, que $\bar{a} \cdot \bar{b} = \overline{ab} = \bar{0}$, para algum par de elementos $\bar{a}, \bar{b} \in \mathbb{Z}_m$. Daí, m divide ab. Mas, como m é primo, então m divide a ou m divide b. Mas essas relações, em termos de classes de equivalência, se traduzem por $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$ Ou seja, se m é primo, então $\mathbb{Z}_m$ não possui divisores próprios de zero e, consequentemente, é um anel de integridade.

1.3 Equações Diofantinas

Chama-se de *Equações Diofantinas* as equações polinomiais com coeficientes inteiros, para as quais só se está interessado em soluções inteiras ou racionais.

As equações Diofantinas das quais nos ocuparemos aqui são de um tipo especial, a saber, são da forma

$$ax + by = n,$$

com a, b e n inteiros.

Nos teoremas a seguir, mostraremos em que condições essa equação admite soluções, e quando existem tais soluções como determiná-las. No que segue, usaremos a notação $a|b$, onde a e b são inteiros, para dizer que a divide b.

Teorema 1.3.1 *A equação $ax + by = n$ admite soluções se, e somente se, $mdc\,(a,b)|n$.*

Demonstração: Suponha que a equação admita uma solução x_0, y_0, isto é, $ax_0 + by_0 = n$. Como $mdc\,(a,b)$ divide a e divide b, segue que também divide $ax_0 + by_0 = n$. Reciprocamente, suponha que $mdc\,(a,b)\,|n$. Então, existe um inteiro t tal que $n = t \cdot mdc\,(a,b)$. Como, pela desigualdade de Bézout, existem inteiros m_0 e n_0 tais que $am_0 + bn_0 = mdc(a,b)$, segue que $n = t \cdot mdc\,(a,b) = (t \cdot m_0) \cdot a + (t \cdot n_0) \cdot b$. Logo, os inteiros $x_0 = t \cdot m_0$ e $y_0 = t \cdot n_0$ formam um par de solução da equação.

Teorema 1.3.2 *Seja x_0, y_0 uma solução particular da equação $ax + by = n$. Tem-se que x, y é uma solução da equação se, e somente se,*

$$x = x_0 + t \cdot \frac{b}{mdc\,(a,b)} \quad e \quad y = y_0 - t \cdot \frac{a}{mdc\,(a,b)}, \tag{1}$$

para $t \in \mathbb{Z}$.

Demonstração: Substituindo x e y da forma (1), na equação, vê-se facilmente que se trata de uma solução. Reciprocamente, se $a = 0$ ou $b = 0$, é claro que toda solução é da forma (1). Vamos chamar $mdc(a,b) = d$. Suponha que $a \cdot b \neq 0$ e x, y é uma solução. Então

$$a \cdot x + b \cdot y = n = a \cdot x_0 + b \cdot y_0.$$

Segue daí que

$$a \cdot (x_0 - x) = b \cdot (y - y_0), \tag{2}$$

e, portanto,

$$\frac{a}{d} \cdot (x_0 - x) = \frac{b}{d} \cdot (y_0 - y).$$

Como $mdc(a/d\,, b/d) = 1$, segue que $(b/d) \mid (x - x_0)$ e $(a/d) \mid (y - y_0)$. Portanto, existem inteiros m e t tais que $y - y_0 = t \cdot (a/d)$ e $x - x_0 = m \cdot (b/d)$. Substituindo estes valores em (2), obtém-se $m = t$. Logo,

$$x = x_0 + t \cdot \frac{b}{d} \quad \text{e} \quad y = y_0 - t \cdot \frac{a}{d}.$$

O conjunto $M_m\,(\mathbb{Z}_n)$ das matizes $n \times n$ com entradas em $\mathbb{Z}_n$, n primo, é um anel com uma unidade, pois $\mathbb{Z}_n$ é comutativo com unidade, $\bar{0}$.

Denotaremos como $U(A)$ o conjunto das unidades de A (elementos invertíveis de A), o conjunto das unidades de $\mathbb{Z}_n$ é denotado por $U(n)$. Para $n = 26$, $U(26)$ representa o conjunto dos elementos invertíveis de $\mathbb{Z}_{26}$.

Teorema 1.3.3 *Uma matriz $A \in M_m(A)$ é invertível $\Leftrightarrow detA \in U(A)$.*

Demonstração: A demonstração desse teorema pode ser vista em Menezes [3].

Pelo Teorema 1.3.3 e pela Proposição 1.2.3 estendemos essa propriedade para o conjunto $M_m(\mathbb{Z}_n)$: dada uma matriz $A \in M_m(\mathbb{Z}_n)$ é invertível $\Leftrightarrow mdc(d,n) = 1$, onde $d = detA$.

Exemplos 1.2.10

1) A matriz $A = \begin{bmatrix} \overline{5} & \overline{14} \\ \overline{3} & \overline{15} \end{bmatrix} \in M_2(\mathbb{Z}_{26})$ é invertível, pois, $d = detA = 33$, e $mdc(33,26) = 1$, isto é, $detA \in U(26)$. Para encontramos a inversa aplicamos $(detA)^{-1} \cdot (adjA)$, que nos dá a matriz A^{-1}, nesse caso $(detA)^{-1}$ em $\mathbb{Z}_{26}$ é 15 e $(adjA) = \begin{bmatrix} \overline{15} & \overline{-14} \\ \overline{-3} & \overline{5} \end{bmatrix}$, fazendo o produto matricial temos:

$$A^{-1} = 15 \begin{bmatrix} \overline{15} & \overline{-14} \\ \overline{-3} & \overline{5} \end{bmatrix} = \begin{bmatrix} \overline{225} & \overline{-210} \\ \overline{-45} & \overline{75} \end{bmatrix} = \begin{bmatrix} \overline{17} & \overline{-2} \\ \overline{-19} & \overline{23} \end{bmatrix}.$$

2) Uma matriz $C = \begin{bmatrix} \overline{16} & \overline{17} \\ \overline{3} & \overline{6} \end{bmatrix}$, não invertível em $M_2(\mathbb{Z}_{26})$, pois $det\ C = 45 \notin U(26)$.

1.4 - Congruências Lineares

Para cumprir com o objetivo principal deste trabalho, vamos precisar da teoria de congruência para resolvermos equações lineares sobre o conjunto $\mathbb{Z}_m$, onde $m > 1$ é um inteiro.

Entendemos como equação linear sobre $\mathbb{Z}_m$ uma equação do tipo $\bar{a} \cdot \bar{x} = \bar{b}$, onde $\bar{a}$ e $\bar{b} \in \mathbb{Z}_m$ e $\bar{x} \in \mathbb{Z}_m$. O intuito é encontrar um número inteiro x que satisfaça tal equação. Se isso for possível, chamamos a classe $\bar{x}$ de solução módulo m desta equação.

Muitas vezes, é útil escrevermos a equação $\bar{a} \cdot \bar{x} = \bar{b}$ na linguagem de congruência, a saber,

$$ax \equiv b \bmod m \qquad (3)$$

para significar que $\overline{ax} = \bar{b}$, isto é, os restos da divisão de ax por m e de b por m são iguais. Em outras palavras, dizer que (2) possui solução é equivalente a dizer que existem inteiros x e t tais que $ax + m\mathrm{t} = b$.

Se x_0 é uma solução de (2) e se $x_1 \equiv x_0 \bmod m$, então $x_1$também é uma solução de $ax \equiv b \bmod m$. Portanto, as soluções da congruência $ax \equiv b \bmod m$ se repartem em classes residuais módulo m.

Se $mdc\ (a,m) = 1$, pela Proposição 1.2.3, segue que $\bar{a}$ é invertível em $\mathbb{Z}_m$. Portanto, a equação (3) tem neste caso uma única solução dada por

$$\bar{x} = (\bar{a})^{-1} \cdot \bar{b}.$$

Em outras palavras, se $(a,m) = 1$, então a congruência (3) tem uma única solução módulo m.

Teorema 1.4.1. *Sejam a, b e m inteiros com $m > 1$. Seja $d = mdc\,(a, m)$. Temos*

(i) *A congruência (3) tem solução se, e somente se, d divide b.*

(ii) *Se d divide b, existem exatamente d soluções distintas da equação (3) módulo m, cujos representantes são*

$$x_0, x_0 + \frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d},$$

onde x_0 é uma solução particular qualquer de (3).

Demonstração: Vamos provar i). A congruência $ax \equiv b \bmod m$ admite solução x se e somente se a equação diofantina $ax + by = b$ admite solução em x e y. Isto implica que d divide b (veja a demonstração da **Proposição 1.2.3**). Agora, vamos provar ii). Seja x_0 uma solução qualquer da congruência $ax \equiv b \bmod m$. Logo, existe y_0 tal que x_0, y_0 é uma solução particular da equação diofantina $ax + by = b$. Pelo **Teorema 1.3.2** da seção anterior, temos que toda solução da equação diofantina $ax + by = b$ é, para $t \in \mathbb{Z}$, da forma

$$x = x_0 + t\frac{m}{d} \quad \text{e} \quad y = y_0 - t \cdot \frac{a}{d}.$$

Isso mostra que toda solução da congruência $ax \equiv b \bmod m$ é da forma

$$x = x_0 + t\frac{m}{d} \qquad , t \in \mathbb{Z}.$$

$$\updownarrow$$

Considere agora as seguintes soluções de (3)

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}. \tag{4}$$

Estas são claramente duas a duas não congruentes módulo m. Além disso, se $x = x_0 + t\frac{m}{d}$ é uma solução qualquer de (3), dividimos t por d e encontramos dois inteiros q e r, com $0 \leq r < d$, tais que $t = mq + r$. Logo,

$$x \equiv x_0 + t\frac{m}{d} \equiv x_0 + r\frac{m}{d} \bmod m.$$

Portanto, x é congruente módulo m a uma das soluções em (4).

2. ORIGEM DA CRIPTOGRAFIA

Criptografia – do grego: *kryptos* (oculto, escondido) e *grafos* (grafia, escrita) surgiu da necessidade de manter o sigilo nas comunicações à distância, protegendo-a contra a ação de espiões. Essa ciência consiste em um conjunto de métodos que permitem codificar um texto, tornando-o ininteligível, de modo que apenas seu destinatário legítimo consiga decodificá-lo.

> "Durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos. Ao mesmo tempo, todos estavam cientes das conseqüências de suas mensagens caírem em mãos erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para forças inimigas. Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler seu conteúdo." ... "em paralelo com o desenvolvimento da esteganografia, houve a evolução da criptografia, derivada da palavra grega kriptos, que significa "oculto". (SINGH, 2008 , p. 1 e 8)

Para melhor compreensão definiremos alguns termos a seguir:

Mensagem original é o texto que queremos enviar. **Mensagem cifrada** é o texto codificado. **Cifrar** ou **criptografar** um texto é o processo em que se converte uma mensagem original em mensagem cifrada.

Quando recuperamos a mensagem original a partir da mensagem cifrada, estamos **decifrando** o texto. Os métodos que utilizamos para codificar e decodificar uma mensagem são chamados de **sistema criptográfico ou criptosistema**. Podemos chamá-los simplesmente de cifra. Em cada sistema criptográfico, usamos números que são as **chaves** para cifrar e decifrar uma mensagem.

Chamamos de **criptosistema de chave secreta** quando a chave de deciframento for igual à de ciframento, ou facilmente podemos obtê-la a partir desta. Caso contrário, é chamado de **criptosistema de chave-pública.**

Chamamos de **criptoanálise** a área que utiliza técnicas usadas para decifrar a mensagem sem qualquer conhecimento da chave de deciframento. Quando acontece isso, dizemos que houve **"quebra do código"**. A criptografia e criptoanálise constituem a **criptologia**. O cripto-sistema deve ser seguro para evitar que a mensagem seja decifrada mesmo que se conheça operações de ciframento e deciframento. Para isso o cripto-sistema deve possuir, entre outras coisas, um número significativo de chaves evitando que a mensagem seja decifrada a partir da aplicação de operação de deciframento com as possíveis chaves.

Estudaremos no capítulo 4 os tipos de criptossistemas de chaves pública e secreta que possuem aplicações da álgebra. Assim, descreveremos como a criptografia evoluiu para os

criptossistemas que conhecemos hoje e sua indispensável contribuição para a segurança da informação e ciframento com as possíveis chaves.

2.1. PRIMEIROS RELATOS DE CRIPTOGRAFIA

Percebemos a presença da criptografia nas civilizações da antiguidade como os egípcios, gregos, hebreus, sírios e hindus nos sistemas de numeração que utilizavam. De acordo com Eves [2], o sistema de numeração grego, conhecido como jônico ou alfabético, cujas as origens se deu por volta de 450 a. C., é um desses sistemas cifrados. É um sistema decimal com 27 caracteres, as 24 letras do alfabeto grego acrescido de três outras obsoletas. Por exemplo, escrevendo o número 13 com esse sistema, o representaríamos da seguinte forma $\alpha\gamma$; 27 como $\beta\zeta$; 452 como $\upsilon\nu\beta$.

Um dos primeiros relatos de transmissão de informações buscando-se o sigilo das informações por meio de códigos, segundo Singh [7], ocorreram também no século V a. C. contados por Heródoto de Helicarnasso, historiador da antiguidade, em sua principal obra Histórias, onde narra os conflitos entre gregos e persas as famosas Guerras Médicas. Heródoto conta o episódio em que o grego Demarato, que vivia exilado na Pérsia, envia uma mensagem aos gregos, informando-lhes dos planos de Xerxes para invadir o país.

Escrevendo em um par de placas de madeiras dobráveis a mensagem e cobrindo-as com cera, enviou-as ao destino, estas seriam raspadas e revelada a mensagem. Xerxes queria atacar a Grécia de surpresa, mas foi impedido por Demarato que revelou aos gregos seus planos.

> "O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os outros gregos." (SINGH, 2008, p. 6).

Outro caso relata que Histau de Mileto com o intuito de fazer com que Aristágora se rebelasse contra o rei persa, escrevendo uma mensagem no couro cabeludo de um escravo e esperando que o cabelo crescesse e em seguida o enviou à Aristágora. Este, chegando à Aristágora, raspou a cabeça, revelando-lhe a mensagem. As formas de se ocultar a mensagem utilizadas por Demarato e Histau são intituladas como estenografia do grego: *steganos*(coberto) e *grapho*(grafia).

Outras formas de estenografia conhecidas que podemos destacar são: a técnica usada na China antiga, que consiste na escrita de uma mensagem secreta em um pedaço de seda fina e depois amassada até formar uma bolinha pequena e, em seguida, coberta com cera e engolida pelo mensageiro.

A escrita sensível criada no século I d. C., que consiste em uma solução à base de ácido cítrico comum em sumo de frutas, vinagre e vinho branco, que era utilizada para enviar mensagens secretas escritas entre linhas de textos comuns que, reagindo com calor, tornavam-se marrons nítida ao remetente. Apesar de parecer simples, a estenografia tem um papel fundamental na criptografia.

Hoje, com técnicas modernas, a estenografia é empregada para vários fins legítimos como identificação de documentos, produtos e objetos, dinheiro, drogas etc. Outra técnica de estenografia é a micropontos, que teve sua origem na Guerra Franco - Prussiana (1870-1871), onde documentos eram microfotografados e enviados por pombo correio aos destinatários que os liam com auxílio de microscópio. Os alemães trouxeram de volta a técnica, utilizando-a na Segunda Guerra Mundial. Microfilmes são miniaturizados até menos de um milímetro de diâmetro e são disfarçados de sinais de pontuação.

Nesses pontos, havia informações secretas que eram transmitidas livremente em cartas e documentos. Apesar de cômoda e segura, a estenografia torna-se frágil, pois não há preocupação em tornar a mensagem ininteligível apenas em ocultá-la. A simples interpretação da mensagem quebra a segurança.

A criptografia não se preocupa em apenas ocultar a mensagem e sim em torná-la ininteligível à alguém que tenha acesso ao texto cifrado. Assim, a criptografia se desenvolveu paralelamente à estenografia, como uma forma alternativa de comunicação secreta. Os métodos de ciframento de mensagens podem ser classificados como: transposição, substituição ou ciframentos compostos.

As **transposições** (ou **simétricas**) simplesmente mudam-se ou permutam-se as letras de uma mensagem, de acordo com um padrão e uma chave previamente estabelecida entre o remetente o destinatário. Nas **substituições** (ou **assimétricas**) as letras da mensagem original são trocadas por outras. Podendo ser **monoalfabéticas** quando não depende da letra na mensagem, isto é, cada letra do texto original é representada por qualquer posição pela mesma substituta, ou **polialfabéticas** quando depende da letra original e da sua posição no texto.

Estes sistemas, conhecidos como **cifras clássicas**, eram utilizados manualmente ou com emprego de dispositivos mecânicos simples. Faremos menção de algumas cifras no capítulo seguinte, devido à sua relevância para o desenvolvimento da criptografia moderna.

Um antigo cripto-sistema de substituição monoalfabética muito utilizado por Júlio César, imperador romano, para comunicar planos de batalha com seus generais, é denominado “Cifra de César”. Para encriptar uma mensagem utilizando esse criptosistema, substitui-se cada letra por outra três posições à frente no alfabeto. Como descrito na tabela abaixo:

Tabela 1.1

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

Temos ainda os ciframentos compostos, que se fundamentam em princípios de transposição e substituição ao mesmo tempo. Veremos no próximo capítulo ciframentos de transposição e de substituição.

Técnicas de estenografia, de transposição e substituição criptográfica já eram utilizadas desde o século V a. C. Técnicas de estenografia e criptografia combinadas aumentavam a segurança da informação.

Os cripto-sistemas de substituição monoalfabética permaneceram por muito tempo como formas de escrita secreta por serem simples e pela segurança que ofereciam na época. Para se quebrar o código era necessário que se verificasse todas as substituições possíveis para as letras. O que demandaria muito tempo, pois isso geraria 26! possibilidades de tabelas para um alfabeto de 26 letras.

> “Foi sua simplicidade e força que fizeram com que a cifra de substituição dominasse a arte da escrita secreta durante o primeiro milênio. Os criadores de códigos tinham desenvolvido um sistema para garantir a segurança das comunicações e portanto não havia necessidade de novos desenvolvimentos — e sem a necessidade, não surgem novas invenções. O ônus caíra sobre os quebradores de códigos, aqueles que tentavam descobrir a cifra de substituição. Será que haveria alguma maneira de um interceptador inimigo descobrir a mensagem cifrada? Muitos estudiosos antigos achavam que a cifra de substituição era indecifrável, graças ao número gigantesco de chaves envolvido, e durante séculos isso pareceu ser verdadeiro. Contudo, os decifradores de códigos iriam, mais tarde, encontrar um atalho no processo de procurar exaustivamente entre todas as chaves possíveis. E no lugar de levar bilhões de anos para se quebrar uma cifra, o atalho revelava o conteúdo da mensagem em questão de minutos. Esta descoberta foi feita no Oriente, e exigiu uma brilhante combinação de lingüística, estatística e devoção religiosa.”(SINGH, 2008. p. 12)

As substituições monoalfabéticas também eram muito utilizadas por eles, e o estudo desses sistemas deu origem à criptoanálise.

Para criptoanalisar as mensagens criptografadas em crifras de substituição monoalfabética os árabes comparavam as frequência das letras na mensagem à frequência relativa das letras no alfabeto, no idioma da mensagem original. Mas esse método demorou a

ser difundido no mundo. Intensificou-se o uso da criptografia na Europa somente no século V, e entre os séculos IX e XIII, ao passo que a criptoanálise começou se desenvolver. A idade das trevas, conhecida como idade média, trouxe um grande atraso intelectual à Europa.

Os mosteiros eram as únicas instituições onde havia um incentivo ao estudo de criptografia, onde monges estudavam a bíblia em busca de significados escondidos nas escrituras sagradas. Eles, de acordo com Singh[7], encontraram nas escrituras um tipo de cifra de substituição hebraica, a *atbsh*, que consiste em tomar-se cada letra e anotar o número de espaços que ela dista no início do alfabeto e, em seguida, substituí-la por uma letra que esteja a uma distância igual do fim do alfabeto. No inglês, o "a" seria substituído pela o "z", o "b" pelo "y", e assim por diante. No Velho Testamento, no livro do profeta Jeremias, nos capítulos 25:26 e 51:41 a palavra "Babel" é substituída por "Sheshach" que é resultado da substituição da letra "beth", a segunda letra no alfabeto hebraico, pela penúltima letra do alfabeto "shin". A segunda letra também "beth" substituída de forma análoga e a última letra de babel é "Iamed", vigésima letra do alfabeto hebraico que é substituída por "kaph" que é a vigésima letra contando-se de trás para frente no alfabeto hebraico. Enquanto os árabes estavam experimentando um enorme avanço intelectual, os europeus ainda estavam se familiarizando com a criptografia. Apenas no século XIV e XV a criptoanálise começou a se desenvolver no ocidente, não se sabe se de forma independente ou se importada dos árabes. Giovanni Soro, Philibert Bobou e Fraçois Viète foram criptoanalistas ocidentais que se destacaram nessa época.

> "Por volta do século XV a criptografia européia era um setor em crescimento. O renascimento das artes, ciências e da educação durante a Renascença produziam o conhecimento necessário para a criptografia, enquanto um crescimento nas maquinações políticas oferecia uma ampla motivação para a comunicação secreta.
>
> ... Ao mesmo tempo em que a criptografia estava se tornando uma ferramenta rotineira da diplomacia, a ciência de criptoanálise começava a aparecer no Ocidente.
>
> ... É bem possível que a criptoanálise tenha sido descoberta independentemente na Europa, mas pode também ter vindo do mundo árabe. ... O primeiro grande criptoanalista europeu foi Giovanni Soro, nomeado secretário de cifras de Veneza em 1506. A reputação de Soro se espalhou pela Itália, e os estados aliados enviavam para Veneza as mensagens interceptadas para serem criptoanalisadas. Até mesmo o Vaticano, provavelmente o segundo maior centro de criptoanálise da Europa na época, enviava para Soro mensagens aparentemente indecifráveis que tinham caído em suas mãos. Em 1526 o papa Clemente VII mandou para ele duas mensagens cifradas e ambas foram devolvidas depois de serem criptoanalisadas com sucesso. ...
>
> ... Em outras partes da Europa, outras cortes também começavam a empregar criptoanalistas habilidosos como Philibert Babou, o criptoanalista do rei Francisco I da França. ... No final do século XVI a França consolidou sua capacidade na solução de códigos com a chegada de François Viète, que tinha um prazer especial em quebrar os códigos espanhóis. Os criptógrafos da Espanha, que pareciam ingênuos comparados com seus rivais do resto da Europa, mal puderam acreditar quando perceberam que suas mensagens eram perfeitamente legíveis para os franceses. O rei Filipe II da Espanha chegou ao ponto de enviar uma petição ao Vaticano, afirmando

> que a única explicação para a criptoanálise de Viète era a de que ele seria “um arquiinimigo compactuado com o demônio”. (SINGH, 2008. p. 20 e 21)

3. TIPOS DE CRIPTOGRAFIA

Neste capítulo, abordaremos alguns tipos de criptografia, sendo elas as cifras de transposição, substituição e ciframento composto – cripto-sistemas de chave secreta, onde a chave de ciframento é a mesma de deciframento ou é facilmente obtida através desta, portanto deve ser ocultada, conhecida apenas pelo remetente e pelo destinatário da mensagem.

3.1 TRANSPOSIÇÕES (OU SIMÉTRICAS)

As transposições consistem em permutar, mudar as letras de uma mensagem reordenando-as de acordo com um determinado esquema, previamente combinado entre o remetente o destinatário da mensagem. É um simples rearranjo das letras no texto da mensagem, gerando anagramas, uma mensagem diferente. Essa reordenação das letras pode ser feita de várias maneiras. É um método inseguro quando utilizado para enviar mensagens curtas como as formadas por uma palavra, pois há um número limitado de maneiras para se reorganizar poucas letras; Entretanto, para mensagens com um número significativo de letras, aumenta-se o número de arranjos, tornando-se impossível obter a mensagem original. O rearranjo das letras ao acaso torna a cifra bastante segura, pois mesmo que a mensagem seja interceptada por um intruso, este não conseguirá decifrá-la mesmo que ela seja pequena. Todavia, para que o método seja eficiente, é necessário, que o rearranjos, das letras deve seguir um fundamento ou rima, combinados entre o remetente e destinatário da mensagem, do contrário seria, inviável decifrar a mensagem até mesmo para o destinatário conhecer o conteúdo da mensagem. (SINHG 2008, p. 7 e 9). Logo, é impossível decodificar a mensagem sem conhecer a chave de codificação.

3.1.1 CERCA DE FERROVIA

Esse cripto-sistema consiste em escrever a mensagem de forma que as letras fiquem alternadas e separadas em duas linhas. Em seguida, escrevemos a primeira linha seguida da segunda, obtendo assim o texto cifrado.

Exemplo 3.1.1

Mensagem original: `alinhe as tropas à direita.`

Codificação da Mensagem:

```
a   i   h   a   t   o   a   a   i   e   t
  l   n   e   s   r   p   s   d   r   i   a
```

Mensagem cifrada: AIHATOAAIETLNESRPSDRIA

Para que o destinatário decifre a mensagem, é necessário apenas reverter o processo.

Podemos utilizar esse sistema para 3 ou mais linhas, encadeá-las alternativamente. Em seguida, trocamos a primeira letra com a segunda, a terceira com a quarta e assim sucessivamente. O número de linhas é a chave para criptografar e descriptografar a mensagem.

Outro exemplo de cifra de transposição é a citale espartano, o primeiro aparelho criptográfico militar do século V a. C., que consiste num bastão de madeira no qual era enrolado uma tira de couro ou pergaminho, onde se escrevia a mensagem; desenrolando a tira de couro as letras parecem sem sentido. Para decifrar a mensagem o receptor, tinha uma bastão semelhante ao do remetente.

> "No ano 404 a.C., Lisandro de Esparta recebeu um mensageiro ensangüentado e ferido, único sobrevivente de um grupo de cinco que partira da Pérsia numa árdua jornada. O mensageiro lhe entregou seu cinturão, que Lisandro enrolou em torno de seu citale para descobrir que o persa Farnabazo estava planejando atacá-lo. Graças ao citale, Lisandro estava preparado para o ataque, e o repeliu. (SINHG, 2008, p. 7)"

A mensagem poderia ainda ser escondida, caracterizando uma técnica também de estenografia, se o mensageiro utilizasse a tira de couro como cinto com a mensagem ocultada pela face dentro, ou como sua imaginação o conduzisse.

Citale Espartano.Fonte:Disponível em:
<http://www.quattropassinellastoria.it>Acesso em: 20/04/2016

3.1.2 CIFRA DE TRANSPOSIÇÃO COLUNAR

Existem várias maneiras de rearranjar as letras de uma mensagem. No entanto, nos ateremos a apenas uma, pois as outras maneiras se baseiam nessa ou em combinações entre elas. Todas utilizam uma chave (uma sequência numérica ou uma palavra) para encriptar a mensagem. Assim, a mensagem que se deseja enviar é escrita linha a linha semelhante a uma matriz. Em seguida as colunas são permutadas de acordo com uma chave (uma sequência de numérica).

> "No método da transposição ocorre apenas um embaralhamento das letras, dispostas em uma ordem pré-determinada para cifrar e decifrar." (BEZERRA, 2010, p. 11).

Para decifrarmos a mensagem, é simples: aplicamos a permutação inversa no texto cifrado obtendo a mensagem original.

Exemplo 3.1.2

Mensagem original: corram para o norte.

Chave: matriz 4×4 e a permutação $(4\ 1\ 2\ 3)$ para as colunas.

Codificação:

1	2	3	4		4	1	2	3
C	O	R	R		R	C	O	R
A	M	P	A	$\longrightarrow$	A	A	M	P
R	A	O	N		N	R	A	O
O	R	T	E		E	O	R	T

Mensagem Cifrada: RCORAAMPNRAOEORT

Decodificação da mensagem: Decodificaremos esta mensagem aplicando a permutação inversa de $(4\ 1\ 2\ 3)$, que é $(3\ 2\ 1\ 4)$.

4	1	2	3			3	2	1	4
R	C	O	R			C	O	R	R
A	A	M	P		$\longrightarrow$	A	M	P	A
N	R	A	O			R	A	O	N
E	O	R	T			O	R	T	E

A ordem das colunas é alterada de acordo com a permutação $(3\ 2\ 1\ 4)$ que é a permutação que nos dá a mensagem original. A coluna 3 da mensagem cifrada vai ser a coluna 2 da mensagem decifrada, a coluna 2 da mensagem cifrada vai ser a coluna 1 da mensagem decifrada e assim por diante. Quando encerrar esse processo, obtemos a mensagem original.

Assim, obtemos a matriz decodificada e, consequentemente, nossa mensagem original.

Mensagem original: corram para o norte.

Outros Exemplos:

Mensagem original: ataquem em Londres.

Chave de Codificação: matriz 4×4 e a permutação $(4\ 3\ 1\ 2)$ para as colunas.

Codificação:

1	2	3	4		3	1	4	2
A	T	A	Q		A	A	Q	T
U	E	M	E	→	M	U	E	E
M	L	O	N		E	M	N	L
D	R	E	S		O	D	S	R

Mensagem Cifrada: AAQTMUEEEMNLODSR

Decodificação da mensagem: Decodificaremos esta mensagem aplicando a permutação inversa de (4 3 2 1), que é (3 4 2 1).

3	1	4	2		3	4	2	4
A	A	Q	T		A	T	A	Q
M	U	E	E	→	U	E	M	E
E	M	N	L		M	L	O	N
O	D	S	R		D	R	E	S

Mensagem Decodificada: ataquem em Londres.

Outra forma de cifrar uma mensagem utilizando cifra de transposição.

Mensagem original: `deposite _quatro_mil_ dólares_ em_ minha_ conta_ nas_ ilhas_ Cayman. Número_ quatro_ sete_ três_ seis.`

Chave de Codificação: 5 1 8 4 2 6 3 7

Dividimos a mensagem em blocos como apresentado e aplicamos a permutação dada, a chave a cada linha do bloco.

d	e	p	o	s	i	t	e
-	q	u	a	t	r	o	-
-	m	i	l	-	d	o	l
a	r	e	s	-	e	m	-
m	i	n	h	a	-	c	o
n	t	a	-	n	a	s	-
i	l	h	a	s	-	c	a
y	m	a	n	-	n	u	m
e	r	o	-	q	u	a	t
r	o	-	s	e	t	e	-

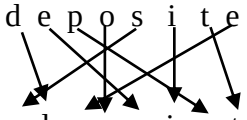
t	r	e	s	-	s	e	i
s							

O bloco de ter o mesmo número de colunas que número de dígitos da chave. Permutamos as colunas de acordo com o indicado, ou seja, a coluna 5 vira a coluna 1, a coluna 1 vira primeira, e assim sucessivamente.

Codificação: A primeira é codificada da seguinte maneira.

1 2 3 4 5 6 7 8

d e p o s i t e



s d e o e i p t

5 1 8 4 2 6 3 7

Mensagem Cifrada: SDEOEIPTT

Para decifrar a mensagem, basta colocar as letras em ordem crescentes dos números correspondentes de cada letra da mensagem.

5 1 8 4 2 6 3 7

s d e o e i p t

d e p o s i t e

1 2 3 4 5 6 7 8

Mensagem Decodificada: DEPOSITE.

3.1.3 CIFRA DE PERMUTAÇÃO PERIÓDICA

A cifra de permutação periódica é definida como embaralhamento de letras de uma mensagem original em blocos de *k* letras seguindo uma permutação escolhida previamente entre o destinatário e remetente da mensagem. Para codificarmos uma mensagem com a cifra de permutação periódica, dividimos a mensagem em blocos de tamanho *k* e consideramos uma permutação $f: A \longrightarrow A$,onde A representa o conjunto de inteiros de 1 a *k.*

A mensagem original

$$m_1 m_2 \cdots m_k \cdots m_{k+1} \cdots m_{2k} \cdots$$

é cifrado como

$$m_{f(1)} m_{f(2)} \cdots m_{f(k)} m_{k+f(1)} \cdots m_{k+f(k)} \cdots$$

Exemplo 3.1.3

Mensagem original: Ataque amanhã em Iorque

Chave: $k=4$ e a permutação

$$i: 1\ 2\ 3\ 4$$
$$f(i): 4\ 2\ 3\ 1$$

Codificação da Mensagem: Ataque amanhã em Iorque

ATAQ EUAM ANHA EMIO RQUE

QTAA MUAE ANHA OMIE EQUR

Mensagem cifrada: QTAAMUAEANHAOMIEEQUR

Para decifrar o destinatário, usará a permutação inversa. Neste exemplo, a permutação inversa de (1 4)(2)(3) em S_4 é dada por (4 1)(2)(3).

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 3 & 1\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$$

Notar que, por exemplo, a imagem de 1 pela composta se obtém da seguinte maneira: $1 \mapsto 4 \mapsto 1$.

Observe que, desta forma, voltamos para a mensagem original.

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$$

Permutamos as letras de cada bloco de quatro letras do texto cifrado de acordo com a permutação inversa encontrada e encontramos a permutação identidade, I, que é a mensagem original.

Mensagem Cifrada: QTAAMUAEANHAOMIEEQUR

Decodificação da Mensagem:

1 2 3 4 1 2 34 1 2 3 4 1 2 34 1 2 3 4

QTAA MUAE ANHA OMIE EQUR

1 2 3 4 1 2 3 4 1 2 3 4 1 2 34 1 2 3 4

ATAQ UEAM ANHA EMIO RQUE

Mensagem decodificada: ATAQUE AMANHA EM IORQUE.

Nas duas cifras, a de transposição colunar e a de permutação periódica, a mensagem é escrita linha por linha, mas na cifra de permutação periódica o texto cifrado é obtido linha por linha e não coluna por coluna. A cifra de permutação periódica possui melhor eficácia do que a de transposição colunar em aplicações computacionais devido este sistema possuir a opção de se poder cifrar cada linha independentemente.

3.2 SUBSTITUIÇÕES

Apresentaremos nesta seção as cifras de substituição monoalfabéticas e polialfabéticas, as formas de encriptar uma mensagem utilizando esses sistemas, as principais características que as diferem e os conceitos matemáticos de álgebra moderna contidos nesses sistemas.

3.2.1 CIFRAS DE SUBSTITUIÇÃO MONOALFABÉTICAS

As substituições complementam as transposições, pois, nestas, cada letra do texto é substituída por uma letra diferente. A cifra de transposição faz com que cada letra se mantenha a mesma, mas muda sua posição, enquanto que a substituição faz com que cada letra mude sua identidade mantendo sua mesma posição, (SINGH, 2008, p. 8). De acordo com MENEZES [3] nas cifras de substituição, monoalfabéticas, cada letra do texto original é substituída sempre pela mesma letra, qualquer que seja a sua posição. Essa substituição pode ser feita de acordo com uma tabela – previamente combinada entre o remetente o destinatário – tomando uma correspondência 1 a 1 entre o alfabeto original e uma versão misturada do mesmo, o alfabeto cifrado. Observe que, para o alfabeto de 26 letras, são 26 possibilidades diferentes de tabelas que podem ser construídas de maneira aleatória, ou a partir de alguma regra, como a **Tabela 1.1** do capítulo 2. Em seguida, discutiremos o conjunto das substituições monoalfabéticas baseado nas transformações afins em $\mathbb{Z}_{26}$, transformações essas, que foram apresentadas no capítulo anterior.

3.2.1.1 CIFRA DE CÉSAR

Conforme descrevemos no capítulo 2, na **Tabela 1.1**, a cifra de César consiste em substituir cada letra de uma mensagem por outra, localizada três posições à frente do alfabeto. Apesar de conhecermos a cifra de César como o deslocamento de cada letra do alfabeto em três posições, qualquer deslocamento entre um e 25 posições nos dá 25 códigos diferentes. Segundo SINGH [7] se considerarmos o alfabeto cifrado como qualquer rearranjo, teremos um número de cifras distintas equivalente a $4 \cdot 10^{26}$. Veremos a seguir um exemplo de generalização para a cifra de César.

Para compreendermos melhor a cifra de César, precisamos conhecer alguns resultados importantes da Álgebra e na Teoria dos Números, que podem ser encontrados em COUTINHO [14] e LEMOS [15], sendo esses os principais:

- Números primos;
- Algoritmo da divisão de Euclides;

- MDC de dois números quaisquer;
- Congruência;
- Inversos multiplicativos em $\mathbb{Z}_m$.

Para encriptar uma mensagem utilizando a cifra de César, como foi dito anteriormente, deslocamos as letras do alfabeto três posições à frente. Considerando o alfabeto cíclico de 26 letras, a letra A do alfabeto é substituída pela letra D, a letra B pela F, e assim sucessivamente. A cada letra associamos um número: ao A o 0, ao B o 1, ao C o 2e assim por diante. Assim, o alfabeto fica ordenado.

Podemos descrever a permutação utilizada na cifra de César matematicamente. Para cada letra do alfabeto, associamos um inteiro do intervalo [0,26). Ao fazermos isso, associamos à *i*-ésima letra do alfabeto o *i*-ésimo número do intervalo [0,26). Estes inteiros são precisamente os restos da divisão por 26, que é o tamanho do conjunto. Assim, podemos associar a cada letra do alfabeto, a um elemento de $\mathbb{Z}_{26}$, isto é, a classe do inteiro associado a essa letra. Logo, a permutação da cifra de César pode ser representada pela função de $\mathbb{Z}_{26}$ em $\mathbb{Z}_{26}$ dada por:

$$\mu(X) = X + \overline{3}$$

Com base na Cifra de César, podemos obter outras cifras usando as permutações dos inteiros módulo n, para algum n natural. Seja S o número de letras do alfabeto β ordenado a ser utilizado. Há uma aplicação bijetora natural entre o alfabeto e os elementos de $\mathbb{Z}_S$, ou seja, cada letra está associada biunívocamente a um elemento de $\mathbb{Z}_S$. Associando $\overline{n}$ a $(n+1)$-ésima letra do alfabeto, para qualquer inteiro n tal que $0 \leq n < S$. Sejam $a, b \in \mathbb{Z}_S$, tal que a possui inverso multiplicativo, veja que $\mu: \mathbb{Z}_S \to \mathbb{Z}_S$ dada por

$$\mu(X) = aX + b$$

é uma bijeção de $\mathbb{Z}_S$. De fato, se $W = aX + b$, então $X = a^{-1}(W - b)$. Logo, para cada elemento W de $\mathbb{Z}_S$, existe um único X em $\mathbb{Z}_S$ tal que $W = \mu(X)$, ou seja, μ é uma permutação.

Os coeficientes a e b são as *chaves* do sistema. Denotamos esse sistema por $\sigma_S(a, b)$. Tendo o conhecimento das chaves a e b, podemos codificar e decodificar as mensagens. Uma vez que para decodificar a mensagem cifrada basta aplicarmos a função inversa μ, que é

$$\mu: \mathbb{Z}_s \to \mathbb{Z}_s$$
$$x \to a^{-1}X - a^{-1}b$$

Observação: Note que para decodificar a mensagem basta que a seja invertível. Isto é verdade, pela Proposição 1.2.3, quando $mdc(a, 26) = 1$.

Exemplo 3.2.1 Utilizando o alfabeto β, considere a permutação μ em $\mathbb{Z}_s$:

$$\mu(X) = \overline{17}X + \bar{2}$$

Veja que $mdc(17,26) = 1$. De acordo com a permutação dada, teremos o seguinte alfabeto.

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
C	T	K	B	S	J	A	R	I	Z	Q	H	Y	P	G	X	E	P	W	P	E	V	M	P	V	L	z

Tabela 3.1

a	b	c	d	e	f	g	H	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
2	19	10	1	18	9	4	17	8	25	16	7	24
C	T	K	B	S	J	E	R	I	Z	Q	H	Y
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
15	6	23	14	5	22	13	4	21	12	3	20	11
P	G	X	O	F	W	N	E	V	M	D	U	L

Cifraremos a mensagem, “Avisem, reforços não serão necessários. Não baixaremos a guarda.” da seguinte maneira. A primeira letra da mensagem é A que, no alfabeto gerado pela permutação, corresponde a letra C; a segunda letra é o V, que não foi alterada, e assim procedemos até codificarmos todas as palavras. Assim, temos a mensagem cifrada

CVIWSYFSJGFKGWPCGWSPCGPSKSWWCPIGWPCGTCIPCPSYGWCEECFBC

Para decifrarmos a mensagem, aplicarmos a permutação inversa de μ que é dada por $\mu^{-1}(X) = a^{-1}(X - b)$. Assim, é necessário encontrarmos o valor de a^{-1} da função. Para isso, utilizando o método de divisões sucessivas determinamos o $mdc(17,26)$ e, consequentemente obtemos meios de resolver a identidade de Bezout relacionada, que nos dará no final do processo o elemento a^{-1}. Assim,

$$26 = 17 \cdot 1 + 9$$
$$17 = 9 \cdot 1 + 9$$
$$9 = 8 \cdot 1 + \underline{1}$$
$$8 = 1 \cdot 8 + 0.$$

Concluímos que, de fato, o $mdc(17{,}26) = 1$. Pela identidade de Bezout, temos que existem x e y inteiros, tais que $17x + 26y = 1$. Resolvendo a equação diofantina $17x + 26y = 1$, temos

$1 = 9 - 8 \cdot 1 = 9 - (17 - 9 \cdot 1) \cdot 1 = 9 - 17 \cdot 1 + (26 - 17 \cdot 1) \cdot 1 \quad = 9 - 17 \cdot 1 + 26 \cdot 1 - 17 \cdot 1 \ = (26 - 17 \cdot 1) - 17 \cdot 1 + 26 \cdot 1 - 17 \cdot 1 = \ 26 - 17 \cdot 1 - 17 \cdot 1 + 26 \cdot 1 - 17 \cdot 1 = 26 \cdot 2 + 17(-1) + 17(-1) + 17(-1) = 26 \cdot \underline{2} + 17 \cdot \underline{(-3)}$

Da equação acima, encontramos $x = -3$ e $y = 2$. No entanto, em $\mathbb{Z}_{26}$, essa equação se reduz a $\overline{17} \cdot \overline{(-3)} = \overline{1}$, pois a outra parcela se anula,($\overline{26}$ em $\mathbb{Z}_{26}$ é igual a $\overline{0}$). Logo, o inverso multiplicativo de $\overline{17}$ em $\mathbb{Z}_{26}$ é $\overline{(-3)}$.

$$\overline{17} \cdot \overline{(-3)} = \overline{1}.$$
$$-3 = 26 \cdot (-1) + 23.$$

O resto da divisão de -3 por 26 é 23. Logo, $\overline{-3} = \overline{23}$. Assim, a^{-1} é igual a $\overline{23}$. Portanto, a permutação inversa é dada por

$$\mu^{-1}(X) = \overline{23}X - \overline{23} \cdot \overline{2}$$
$$\mu^{-1}(X) = \overline{23}X - \overline{46}$$
$$\mu^{-1}(X) = \overline{23}X - \overline{20}$$

Agora, decodificando a mensagem que ciframos anteriormente, a primeira letra da mensagem é o `C`, aplicamos o correspondente número da letra `C` de acordo com Tabela 3.1 na função μ^{-1}. Logo,

$$\mu^{-1}(2) = \overline{23} \cdot 2 - \overline{20} = \overline{26}.$$

Obtemos o elemento $\overline{26}$ que em $\mathbb{Z}_{26}$ é igual a $\overline{0}$, que corresponde a letra `A`. A letra `V` e `I`, não foram alteradas. A letra `W`, cujo número correspondente é `22`, aplicando na função

$$\mu^{-1}(22) = \overline{23} \cdot 22 - \overline{20} = \overline{486} = \overline{18}.$$

Obtendo o $\overline{18}$ que corresponde a letra `S`. A letra `S` cujo número correspondente é `18`, aplicado na função μ^{-1} obtemos o $\overline{4}$, que corresponde a letra `E`. A letra `Y` cujo número correspondente é 24, aplicado na função μ^{-1} obtemos o $\overline{12}$, que corresponde a letra `M`, e assim por diante. Feito esse processo com todas as letras da mensagem cifrada, decodificamos a mensagem. Obtendo assim, a seguinte sequência numérica

0 21 8 18 4 12 17 4 5 14 17 2 14 18 13 0 14 18 4 17 0 14 13 4 2 4 18 18 0 17 8 14 18 13 0 14 1 0 8 23 0 17 4 12 14 18 0 6 20 0 17 3 0

Substituindo cada número por sua letra correspondente. Obtemos a mensagem original.

"Avisem, reforços não serão necessários. Não baixaremos a guarda."

Um dos meios de criptoanalisar uma mensagem cifrada com a cifra de César é testar as possíveis chaves a e b, visto que $\mathbb{Z}_{26}$ possui 12 elementos invertíveis e 26 valores para b, dando um total de 312 possibilidades permutações do alfabeto. Outra maneira é por análise de frequência das letras da mensagem cifrada. Observando a ocorrência das letras C e S na mensagem podemos perceber que elas aparecem com maior ocorrência.

CVIWSY FSJGFKGW PCG WSPCG PSKSWWCPIGW PCG TCIPCPSYGW C EECFBC

As letras que aparecem com maior frequência em português são o A, E e O. Podemos supor que as letras C e S foram trocadas por A e E, respectivamente. Admitindo-se que o criptoanalista conheça o sistema de criptografia utilizado pelo remetente, mas não conheça as chaves, este pode obtê-las a partir da resolução do sistema de equação linear em $\mathbb{Z}_{26}$.

$$\begin{cases} \bar{0}a + b = \bar{2} \\ \bar{4}a + b = \overline{18} \end{cases}$$

A primeira equação mostra que o A foi substituído pelo C. E na segunda, que o E foi substituído pelo S. Subtraindo a segunda da primeira, temos

$$\bar{4}a = \overline{16}$$

reduzindo até acharmos como a é escrito

$$\begin{aligned} 4a - 16 &= 26k \\ 4a &= 26k + 16 \\ 2a &= 13k + 8 \qquad (k = 2i) \\ 2a &= 26i + 8 \quad a = 13i + 4 \quad i \in \mathbb{Z} \end{aligned}$$

se $i = 2n$, então $a = \bar{4}$ e se $i = 2n + 1$, $a = \overline{17}$

Portanto, $a = \bar{4}$ ou $a = \overline{17}$. Logo, $(a, b) \in \{(\bar{4}, \bar{2}), (\overline{17}, \bar{2})\}$ que são as soluções do sistema. Verificamos agora com qual destes dois pares de chaves podemos decifrar a

mensagem. É fácil ver que a solução é o segundo par, que define a função μ. Como já encontramos anteriormente os valores de a^{-1} e b, basta aplicarmos na função

$$\mu^{-1}(X) = (a^{-1}, -a^{-1}b)$$

e teremos a mensagem original

$$\mu^{-1}(X) = (a^{-1}, -a^{-1}b)$$
$$\mu^{-1}(X) = a^{-1}X + (-a^{-1}b)$$
$$\mu^{-1}(X) = a^{-1}X - a^{-1}b$$
$$\mu^{-1}(X) = a^{-1}(X - b)$$
$$\mu^{-1}(X) = \overline{23}(X - \bar{2})$$
$$\mu^{-1}(X) = \overline{23}X - \overline{20}$$

3.2.2 CIFRAS DE SUBSTITUIÇÃO POLIALFABÉTICAS

A cifras de substituição polialfabéticas, de acordo com LUIZ [11] é a conjunção de várias cifras de substituição monoalfabéticas.

3.2.2.1 CIFRAS DE HILL

Nas cifras polialfabéticas, uma mesma letra na mensagem original pode ser substituída por letras diferentes o que dificulta o processo de decifração por análise de freqüência, embora possa ser criptoanalisada por recursos de álgebra linear. Apresentaremos a seguir as cifras de Hill, em que a substituição é feita em blocos de n letras e codificadas através de processos de transformação matricial.

A codificação em cifras de Hill é feita da seguinte maneira: a mensagem original é divida em blocos de comprimento n de letras, de números equivalentes a $(m_1, m_2, \dots, m_n)$, dado pelo alfabeto mencionado anteriormente, o alfabeto β (ao A o 0, ao B o 1 , ao C o 2, ... , Z ao 25). As letras do texto cifrado $(c_1, c_2, \dots, c_n)$ são, no nosso caso, em $\mathbb{Z}_{26}$, onde cada c_i é combinação linear de $(m_1, \dots, m_n)$, dado um i qualquer tal que $1 \leq i \leq n$, ou seja

$$c_1 = a_{11}m_1 + \cdots + a_{1n}m_{1n}$$
$$c_2 = a_{21}m_1 + \cdots + a_{2n}m_{2n}$$
$$c_n = a_{n1}m_1 + \cdots + a_{nn}m_n,$$

com $a_{ij} \in \mathbb{Z}_{26}$.

Em notação matricial, temos

$$C = AM$$

onde

$$C = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}, A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \; e \; M = \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix}$$

são matrizes com entradas em $\mathbb{Z}_{26}$.

Para decifrarmos uma mensagem em cifra de Hill, basta multiplicarmos a equação em ambos os membros por A^{-1}, matriz inversa de A, ou seja, $A^{-1} \times C = A^{-1} \times AM$, encontrando a $M = A^{-1} \times C$, que nos dá a mensagem decifrada. Mas, para que a mensagem seja decifrada, é necessário que a matriz A seja inversível, ou seja, $mdc(detA, 26) = 1$, conforme resultado que pode ser visto no capítulo 2.

Exemplo 3.2.2

Admitindo $n = 2$, considere:

Mensagem original: `combate em Montese artilharia.`

Chave de Ciframento: $A = \begin{bmatrix} 5 & 14 \\ 3 & 15 \end{bmatrix} \in M_2(\mathbb{Z}_{26})$

Codificação da Mensagem:

`CO MB AT EE MM ON TE SE AR TI LH AR IA`

Substituindo cada letra pelo seu número correspondente no alfabeto (ao A o 0, ao B o 1 , ao C o 3, ..., ao Z o 25), temos:

2 14 12 1 0 19 4 4 12 12 14 13 19 4 18 4 0 17 19 8 11 7 0 17 8 0

Escrevemos como matriz coluna cada par de números correspondente a cada par de letras, e fazemos o produto dela com a matriz A, obtendo as primeiras letras do texto cifrado.

$$C = AM = \begin{bmatrix} 5 & 14 \\ 3 & 15 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} 5 \cdot 2 + 14 \cdot 14 \\ 3 \cdot 2 + 15 \cdot 14 \end{bmatrix} = \begin{bmatrix} 24 \\ 8 \end{bmatrix}$$

que corresponde as letras `YI` do alfabeto citado anteriormente.

As próximas letras são cifradas da mesma maneira:

$$C = AM = \begin{bmatrix} 5 & 14 \\ 3 & 15 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \cdot 12 + 14 \cdot 1 \\ 3 \cdot 12 + 15 \cdot 1 \end{bmatrix} = \begin{bmatrix} 22 \\ 24 \end{bmatrix}$$

que são exatamente as letras WY que correspondem a esses números no alfabeto dado anteriormente. Criptografamos os demais pares de letras de forma análoga, até o ultimo par.

24 8 22 24 6 25 24 20 20 8 18 3 21 13 16 10 4 21 25 21 23 8 4 21 14 24

que correspondem as letras:

WY GZ YU UI SD VN QK EV ZV XI EV OY

Mensagem Cifrada: WYGZYUUISDVNQKEVZVXIEVOY

Para decodificarmos a mensagem, utilizamos a matriz A^{-1} . Dada uma matriz A, com $detA \neq 0$, A é inversível com $A^{-1} = (detA)^{-1}(adjA)$, onde a $adjA$ é a matriz transposta dos cofatores A, denominada $Matriz\ Adjunta$.

A matriz cofatores de A, é $\bar{A} = \begin{bmatrix} 15 & -3 \\ -14 & 5 \end{bmatrix}$.Então, $adj\ A = \begin{bmatrix} 15 & -14 \\ -3 & 5 \end{bmatrix}$.

Multiplicando $adj\ A$ pelo $(detA)^{-1}$ em $\mathbb{Z}_{26}$, obtemos a matriz decodificadora.

Temos que, $detA = 33$ que em $\mathbb{Z}_{26}$ é igual a 7. Então $detA = 7$ e $\overline{7^{-1}} = \overline{15}$ em $\mathbb{Z}_{26}$.

Portanto, $A^{-1} = 15\begin{bmatrix} 15 & -14 \\ -3 & 5 \end{bmatrix} = \begin{bmatrix} 225 & -210 \\ -45 & 75 \end{bmatrix} = \begin{bmatrix} 17 & -2 \\ -19 & 23 \end{bmatrix}$.

Decodificando o primeiro par de letras, temos:

$$\begin{bmatrix} 17 & -2 \\ -19 & 23 \end{bmatrix}\begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} 17 \cdot 24 + (-2) \cdot 8 \\ -19 \cdot 24 + 23 \cdot 8 \end{bmatrix} = \begin{bmatrix} 2 \\ -12 \end{bmatrix} = \begin{bmatrix} 2 \\ 14 \end{bmatrix},$$

substituindo os números pelas letras correspondentes, voltamos ao primeiro par de letras CO. De forma análoga, obtemos os outros pares de letras. Feito isso, obtemos a mensagem original.

COMBATE EM MONTESE ARTILHARIA.

4. CONSIDERAÇÕES FINAIS

Ao estudarmos criptografia percebemos a riqueza que esta ciência possui e como ela impulsionou o homem a criar mecanismos para se comunicar de forma segura, e consequentemente proporcionou o desenvolvimento das tecnologias, essenciais à vida moderna. A importância da criptografia na Segunda Guerra Mundial, as contribuições para o avanço científico e tecnológico que a criação de quartéis generais para pesquisas em criptografia proporcionaram à humanidade, como o Quartel-General de Comunicações do Governo britânico (GCHQ — Government Communications Headquarters), a Agência Nacional de Segurança (NSA — National Security Agency) norte-americana atualmente desenvolve pesquisas secretas. As contribuições de Turing para a computação desenvolvendo a *Collossus*, e mais tarde ACE (Automatic Computing Engine), a idéia de as máquinas pensam, sendo o precursor da inteligência artificial. O desenvolvimento intelectual, nas artes, na ciência e na política, na sociedade islâmica, se deu devido ao uso da criptografia e a invenção da criptoanálise. A importância utilização da criptografia atualmente, por empresas que necessitam de uma criptografia segura para suas transações financeiras, via internet. Percebemos a importância da matemática, como ciência, para o progresso cientifico e tecnológico atual. Resultados da álgebra e da teoria dos números que contribuíram para o avanço da criptografia. Assim, nesse trabalho, restringimos nossa pesquisa aos sistemas de criptografia Clássica ou criptografia de chave secreta: cifras de transposição e substituição. Apesar desses sistemas serem considerados ultrapassados, devido à pouca segurança que oferecem, optamos por esses métodos por sua importância para à criptografia moderna. Recomendamos a futuros trabalhos, pesquisas no campo da criptografia de chave pública, a mais conhecida atualmente por ser considerada inquebrável, a criptografia RSA, e criptografias de sistemas compostos, como DES.

REFERÊNCIAS

[1] DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra moderna:** volume único. 4. ed. reform. São Paulo: Atual, 2003.

[2] HOWARD, Anton; RORRES, Chris. **Álgebra Linear com aplicações**. trad.Claus Ivo Doering. 8. ed. Porto Alegre: Bookman, 2001.

[3] MENEZES, Roselaine de. **Criptografia e Álgebra** – UFMG, 2003. Disponível <http:// www.mat.**ufmg**.br >. Acesso em: 01 abril. 2015.

[4] EVES, Howard. **Introdução à história da matemática** – trad.: Hygino H. Domingues – Campinas, SP: Editora da UNICAMP, 2004.

[5] BOYER, Carl B. **História da matemática** – revista por Uta C. Merzbach; trad.: Elza F. Gomide – 2. ed. – São Paulo: Blücher, 1996.

[6] CRUZ, Edilson F. da. **A Criptografia e eu papel na Segurança da Informação e das Comunicações (SIC)– Retrospectiva, Atualidade e Perspectiva -** Brasília –DF ,2009. Disponível <http: ww.d**sic**.planalto.gov.br >. Acesso em: 21 março 2016.

[7] SINGH, Simom, **O livro dos Códigos**. Rio de Janeiro, Record, 2008.

[8] HEFEZ, Abramo, **Curso de Álgebra, volume 1 (3° edição).** Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2002.

[9] GONÇALVES, Alfredo, **Introdução a Álgebra**, Rio de Janeiro: IMPA, 2006.

[10] SANTOS, Reginaldo J, **Geometria analítica e álgebra linear.** Belo Horizonte, UFMG, 2001.

[11] LUIZ, José dos Santos. **A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica.** Bahia: UFBA, 2013. Disponível em <http: www.bit.profmat-sbm.org.br >. Acesso em: 28 agost. 2016.

[12] ARNALDO, Garcia, LEQUAIN, Yves, **Elementos de álgebra**, 3 ed. Rio de Janeiro: IMPA, 2005.

[13] BEZERRA, Débora de Jesus, MALAGUTTI, Pedro Luiz, RODRIGUES, Vânia Cristina da Silva. **Aprendendo Criptologia de Forma Divertida**. [S.l:sn], UFPB, 2010. Disponível em <http:// www.mat.ufpb.br/ >. Acesso em: 28 agost. 2016.

[12] ALBERTO, Luis de Moraes Barbosa. FERNANDO, Luis B Braghetto. LOTIERSO, Marcelo Brisqui, CRISTINA, Sirlei da Silva ***RSA Criptografia Assimétrica e Assinatura Digital*.** Campinas. UNESP, 2003. Disponível em < www.bibliotecadigital.unicamp.br >. Acesso em: 17 agost. 2016.

[14] COUTINHO, S. C. **Números Inteiros e Criptografia RSA**, 2. ed. Rio de Janeiro: IMPA, 2003.

[15] LEMOS, Manuel. **Criptografia, Números Primos e Algoritmos 4° edição.** UFPE, IMPA 2010. Disponível em <https: www.impa.br >. Acesso em: 17 agost. 2016.

[16] LEAVITT, David. **O Homem que Sabia Demais Alan Turing e a Invenção do Computador**, trad. Samuel Dirceu. 1. ed. Novo Conceito: Riberão Preto São Paulo, 2011.

[17] STRATHERN, Paul. **TURING E O COMPUTADOR em 90 minutos**, trad. Maria Luiza X. de A. Borges. 1. ed. Jorge Zahar: Rio de Janeiro, 2000.