UNIVERSIDADE FEDERAL DO TRIÂNGULO MINEIRO

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

EDSON MARQUES DA COSTA JÚNIOR

A CRIPTOGRAFIA COMO FERRAMENTA DE INCENTIVO AO ESTUDO DA MATEMÁTICA

Uberaba-MG
2014

Catalogação na fonte: Biblioteca da Universidade Federal do Triângulo Mineiro

C873c

Costa Júnior, Edson Marques da
A criptografia como ferramenta de incentivo ao estudo da matemática / Edson Marques da Costa Júnior. -- 2014.
73 f. : il., graf., tab.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) -- Universidade Federal do Triângulo Mineiro, Uberaba, MG, 2014
Orientador: Prof. Dr. Rafael Peixoto

1. Criptografia. 2. Matemática - Estudo e ensino. 3. Congruências e restos. 4. Aritmética. I. Peixoto, Rafael. II. Universidade Federal do Triângulo Mineiro. III.Título.

CDU 511.11

EDSON MARQUES DA COSTA JÚNIOR

A CRIPTOGRAFIA COMO FERRAMENTA DE INCENTIVO AO ESTUDO DE MATEMÁTICA

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional-PROFMAT, como parte das atividades para obtenção do título de Mestre em Matemática da Universidade Federal do Triângulo Mineiro-UFTM, Departamento de Matemática.

Uberaba-MG
2014

EDSON MARQUES DA COSTA JÚNIOR

A CRIPTOGRAFIA COMO FERRAMENTA DE INCENTIVO AO ESTUDO DE MATEMÁTICA

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional-PROFMAT, da Universidade Federal do Triângulo Mineiro, como parte das atividades para obtenção do título de Mestre em Matemática.

17 de Dezembro de 2014

Banca Examinadora

Prof. Dr. Rafael Peixoto
Orientador
Universidade Federal do Triângulo Mineiro

Prof. Dr. Leandro Cruvinel Lemes
Universidade Federal do Triângulo Mineiro

Prof. Dr. Alonso Sepúlveda Castellanos
Universidade Federal de Uberlândia

Dedico este trabalho ao triângulo que sustenta minha vida: Natalia (meu amor), Lucimar (a melhor mãe do mundo) e Edson (in memoriam) pelos valores ensinados...

Agradecimentos

Ao término deste trabalho, deixo aqui meus sinceros agradecimentos:

- A Deus, por ter me dado a oportunidade de estar aqui. Sem ele nada seria possível. Meu ALFA e o meu ÔMEGA, minha força e inspiração, consolo e fortaleza.
- À minha esposa, pela paciência, amor, carinho e compreensão nos momentos difíceis. Companheira, amiga e amante. Meu porto seguro, sem ela não seria metade do que sou hoje. Sou muito feliz por tê-la ao meu lado.
- À minha mãe, que me ensinou a viver a vida com dignidade sempre me direcionando para o caminho certo; mulher guerreira e batalhadora, esforçando-se para me dar o que de mais precioso existe: EDUCAÇÃO.
- Ao meu pai, que me mesmo não estando mais presente, ensinou-me os principais valores da vida. Permanecerá sempre vivo em mim.
- À minha irmã, mulher doce e compreensível, apoiando-me e me dando forças nos momentos mais difíceis.
- A todos os meus amigos que me apoiaram direta ou indiretamente. Em especial, Gustavo, Geanne, Denis, Marcelo, Henderson, Fernando, Larissa e Rosa, pessoas sempre presentes no meu dia a dia, meu muito obrigado.
- Aos meus familiares, que sempre me apoiaram nos momentos mais difíceis.
- Aos companheiros de classe que fizeram parte desse momento ímpar.
- Agradeço ao meu Orientador, Prof. Dr. Rafael Peixoto, pelos ensinamentos e pela paciência.
- Agradeço aos professores Prof. Dr. Leandro Cruvinel Lemes e o Prof. Dr. Alonso Sepúlveda Castellanos por terem aceitado o convite para fazerem parte da minha banca.
- À Sociedade Brasileira de Matemática que na busca da melhoria do ensino de Matemática na Educação Básica, viabilizou a implementação do PROFMAT.

"Sempre me pareceu estranho que todos aqueles que estudam seriamente esta ciência acabam tomados de uma espécie de paixão pela mesma. Em verdade, o que proporciona o máximo de prazer não é conhecimento e sim a aprendizagem, não é a posse, mas a aquisição, não é a presença, mas o ato de atingir a meta."(*AlbertEinstein*)

Resumo

Este trabalho tem por objetivo incentivar o estudo da matemática através da criptografia. Verificando a frequente falta de interesse dos discentes pela matéria, o estudo da criptografia pode auxiliar no desenvolvimento cognitivo dos alunos no Ensino Médio tornando a matemática mais atraente. Para a realização desse, foi necessária a introdução de conceitos básicos da Teoria dos Números de forma a auxiliar nos estudos de técnicas criptográficas desde rudimentares como Cifras de deslocamento, Cifrários por Substituição, Cifrário Bifendido de Delastelle, Transposição Colunar e Máscara de Matias Sandorf até métodos mais avançados como Cifras afim e Cifras de Hill. Na parte final do trabalho, foi descrito um minicurso no qual a abordagem principal é a introdução da Teoria dos Números no Ensino Médio de uma maneira lúdica, dessa forma, os conceitos envolvendo técnicas de cifragem foram primordiais.

Palavras chave: Congruência, Aritmética das Classes Residuais, Criptografia.

Abstract

The present work aims at encouraging the study of mathematics through encryption. Regarding the frequent lack of interest of students in the subject, the study of encryption can aid cognitive development of students in high school, making Maths more attractive. To achieve this, it was necessary to introduce basic concepts of the Number's Theory so as to help in the study of cryptographic techniques, be them rudimentary ones, such as Displacement Cypher, Substitution Cypher, Delastelle's Bigapped Cypher, Columnar Transposition and Matias Sandorf's Mask, or be them more advanced methods, such as Related Cypher or Hill's Cypher. In the final part of the article, we described a short course in which the main approach is the introduction of Number's Theory in high school in a playful way, thus, concepts involving encryption techniques were paramount.

Keywords: congruence, Residual Classes, Arithmetic, Encryption.

Conteúdo

Capítulo 1

Introdução

A Criptografia é o estudo de métodos, cada vez mais sofisticados, para enviar mensagens secretas ou codificadas como pode-se verificar em [8] e [3]. Como se ver ao longo deste trabalho, essa técnica não seria aprimorada sem a utilização da Teoria dos Números, área da Matemática vista por muitos como meramente abstrata e sem nenhuma aplicabilidade no mundo real.

Partindo do princípio de que a criptografia é um assunto interessante para muitos no contexto atual, acredita-se que sua utilização em sala de aula possa despertar maior interesse dos alunos. Trazendo esta discussão para dentro dos perímetros da escola, poderemos associá-la com conteúdos matemáticos, facilitando, dessa forma, a aprendizagem destes.

Observando a falta de interesse por parte de alguns alunos da Educação Básica, em relação à disciplina de Matemática, por não observarem a utilidade de determinadas matérias no dia a dia, ou em áreas específicas, desenvolveu-se esse trabalho cujo objetivo principal é mostrar como a criptografia pode contribuir para a fixação de conteúdos vistos em sala de aula, além de auxiliar na implementação de matérias de nível superior no Ensino Médio.

Esse trabalho foi elaborado basicamente em três pilares:

- Introdução à Teoria dos Números.
- Introdução à Criptografia e seus diferentes métodos.
- Criptografia em sala de aula.

A fim de proporcionar uma visão geral do trabalho, apresentamos uma breve descrição dos assuntos abordados em cada um dos capítulos. No segundo capítulo, serão introduzidos alguns conceitos primitivos relacionados à Teoria dos Números. Estudaremos resultados sobre congruência, congruências lineares e Aritmética das Classes Residuais baseados em [1] que nos fornecerão ferramentas para estudos sobre criptografia.

No terceiro capítulo, serão descritos alguns métodos para criptografar mensagens com a utilização desde processos rudimentares como a Cifra de Deslocamento, Cifra de Cesar, Cifrário Bifendido de Delastelle, Transposição Colunar, Permutação e a Máscara de Matias Sandorf, até processos mais avançados como a Cifra de Hill e a Cifra afim. Mostraremos como codificar e decodificar mensagens por esses métodos, além de mostrar uma abordagem matemática sobre cada uma dessas.

No quarto capítulo, apresentaremos uma descrição sobre o minicurso realizado com os alunos do Ensino Médio de uma escola de Uberlândia. Esse capítulo inicia-se mostrando a importância da Criptografia no dia a dia e em um determinado contexto histórico, passando desde a introdução à Teoria Básica dos Números até alguns métodos criptográficos vistos no capítulo 2. A observação do relato dos alunos é importante para o desenvolvimento da atividade proposta, bem como para fornecer maior dinâmica ao trabalho realizado.

Espera-se que este trabalho sirva de apoio a professores da rede básica de educação para a elaboração de roteiros de aplicação de atividades em sala de aula para alunos do Ensino Médio. A abordagem de temas como a criptografia para a introdução de conteúdos até então abstratos, pode facilitar o processo de ensino-aprendizagem dos discentes e, dessa forma, desenvolver maior interesse dos estudantes não só sobre o assunto em questão, como também pela matéria lecionada.

Capítulo 2

Teoria dos Números

Neste capítulo estudaremos os principais conceitos relacionados à **congruência** para que possamos ter um melhor embasamento teórico para o posterior estudo sobre Criptografia. Essas informações nos dará suporte para afirmações sobre as diferentes formas de cifras.

2.1 Congruência

Inicialmente demonstraremos o teorema da divisão Euclidiana, princípio básico para todo nosso estudo.

Teorema 2.1.1 *Sejam a e b dois números naturais com $0 < a < b$. Existem dois únicos números naturais q e r tais que*

$$b = a \cdot q + r, \ com \ r < a.$$

Dem. Sem perda de generalidade, suponha que $b > a$ e considere, os números

$$b, b-a, b-2a, ..., b-n \cdot a, ..$$

Pela *Propriedade da Boa Ordem* [1], o conjunto S formado pelos elementos acima tem um menor elemento $r = b - q \cdot a$. Vamos provar que r tem a propriedade requerida, ou seja, que $r < a$.

Se $a|b$ ou seja, se b é divisível por a, então $r = 0$, assim a demonstração está concluída. Se, por outro lado, $a \nmid b$ ou seja, b não é divisível por a, então $r \neq a$, e, portanto, basta mostrar que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número natural $0 < c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - q \cdot a$, teríamos

$$c = b - (q+1) \cdot a \in S, \ com \ c < r$$

contradição com o fato de r ser o menor elemento de S.

[1] Todo subconjunto não vazio do conjunto dos números naturais possui um menor elemento.

Portanto, temos que $b = a \cdot q + r$ com $r < a$, o que prova a existência de q e r.

Agora, vamos provar a unicidade. Note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a.

Sejam $r = b - a \cdot q$ e $r' = b - a \cdot q'$, com $r < r' < a$, assim $r' - r = b - a \cdot q' - (b - a \cdot q) = a \cdot (q - q')$. Como $q - q' \geq 1$, segue que $r' - r \geq a$ o que implica que $r' \geq r + a \geq a$, absurdo. Portanto, $r = r'$.

Daí segue-se que $b - a \cdot q = b - a \cdot q'$, o que implica que $a \cdot q = a \cdot q'$ e, portanto, $q = q'$. ■

Definição 2.1.2 *Seja m um número natural diferente de zero. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se:*

$$a \equiv b \mod m.$$

Exemplo 2.1.3 *Vejamos:*

- $10 \equiv 7 \mod 3$ *já que os restos da divisão de* 10 *e* 7 *por* 3 *são iguais a* 1.
- $22 \equiv 34 \mod 4$ *já que os restos da divisão de* 22 *e* 34 *por* 4 *são iguais a* 2.

É importante observar que $a \equiv b \mod 1$ quaisquer que sejam $a, b \in \mathbb{Z}$ já que o resto da divisão de todos os números inteiros por 1 é sempre nulo.

Decorre dessa definição algumas propriedades imediatas que destacaremos agora:

Proposição 2.1.4 *Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que:*

1. $a \equiv a \mod m$,
2. *se* $a \equiv b \mod m$, *então* $b \equiv a \mod m$,
3. *se* $a \equiv b \mod m$ *e* $b \equiv c \mod m$, *então* $a \equiv c \mod m$.

A teoria das congruências foi apresentada rigorosamente por Carl Friedrich Gauss, mais conhecido pelo seu último nome, aos vinte e quatro anos de idade no seu famoso livro Disquistiones Artihmaticae de 1801 onde só foi traduzido para o inglês em 1966 já que o mesmo era alemão.

Figura 2.1: Carl Friedrich Gauss[1]

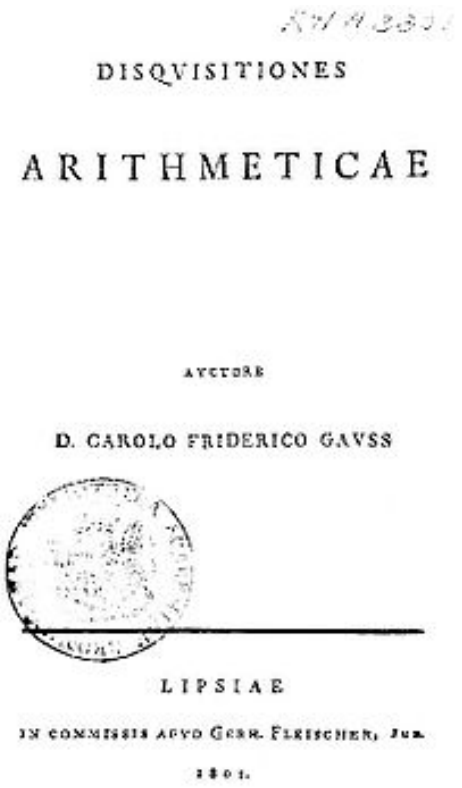


Figura 2.2: Disqvisitiones Arithmeticae[2]

Proposição 2.1.5 *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \mod m$ se, e somente se, $m|(b-a)$.*

Dem.

Pela divisão euclidiana, temos que $a = mq + r$ e $b = mq' + r'$ com $r < m$ e $r' < m'$. Assim, podemos observar que,

$$b - a = m(q - q') + (r' - r)$$

Logo, $a \equiv b \mod m$ se, e somente se, $r = r'$, o que equivale a dizer que $m|(b-a)$, já que $|r - r'| < m$.

■

Proposição 2.1.6 *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$*

1. *Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a + c \equiv b + d \mod m$.*

[1] figura retirada de http://www-history.mcs.st-and.ac.uk/PictDisplay/Gauss.html

[2] figura retirada de http://pt.wikipedia.org/wiki/Disquisitiones_Arithmeticaemediaviewer/File : Disqvisitiones − 800.jpg

2. $a \equiv b \mod m$ *e* $c \equiv d \mod m$*, então* $ac \equiv bd \mod m$*.*

Dem.

Como $a \equiv b \mod m$ e $c \equiv d \mod m$, podemos escrever que $m|b-a$ e $m|d-c$ logo, podemos observar que,

1. $m|(b-a)+(d-c)$ e portanto, $m|(b+d)-(a+c)$ o que prova o primeiro item.

2. basta observar para o segundo item que $bd-ac = d(b-a)+a(d-c)$ e concluir que $m|bd-ac$.

■

Corolário 2.1.7 *Para todos* $n \in \mathbb{N}$*,* $a, b \in \mathbb{Z}$*, se* $a \equiv b \mod m$*, então tem-se que* $a^n \equiv b^n \mod m$*.*

Utilizando a notação de congruência, podemos enunciar o Pequeno teorema de Fermat antes disso, enunciaremos um lema como se segue:

Lema 2.1.8 *Seja p um número primo. Os números* $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$ *, onde* $0 < i < p$*, são todos divisíveis por p.*

Dem.

É importante observar inicialmente que $\binom{p}{i}$ sempre será um número natural. Vejamos que:

$$\binom{p}{i} = \frac{p(p-1).(p-2)...(p-i+1)}{i!}$$

Como p é primo e $p > i$, temos que $mdc(i!, p) = 1$. Logo $i!|(p-1).(p-2)...(p-i+1)$, isto é, $\dfrac{(p-1).(p-2)...(p-i+1)}{i!}$ é natural. Portanto,

$$\binom{p}{i} = p\frac{(p-1).(p-2)...(p-i+1)}{i!}$$

o que ocasiona que $p|\binom{p}{i}$.

■

Em posse das proposições, lema e corolários anteriores, segue o Pequeno teorema de Fermat.

Teorema 2.1.9 ***Pequeno Teorema de Fermat***

Dado um número primo p, tem-se que p divide o número $a^p - a$*, para todo* $a \in \mathbb{Z}$*.*

Dem.

Iremos mostrar por indução sobre a. Primeiramente provaremos para $a = 0$ o que é óbvio já que $p|0$. Agora, suponha o resultado válido para a ou seja $a^p \equiv a \mod p$. Provaremos válido para $a+1$ ou seja, $(a+1)^p \equiv a+1 \mod p$. Por binômio de Newton, temos o seguinte resultado.

$$(a+1)^p - (a+1) = \overbrace{a^p - a}^{p|} + \overbrace{\binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a}^{p|}.$$

Mas, pelo hipótese de indução temos que $p|(a^p - a)$ e pelo lema acima,

$$p|\left(\binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a\right) \Longrightarrow (a+1)^p \equiv a+1 \mod p,$$

o que nos fornece o resultado que queríamos. ■

Um outro método de se escrever o pequeno teorema de Fermat, é dado como segue abaixo.

Teorema 2.1.10 ***Pequeno Teorema de Fermat***

Se p é primo e $a \in \mathbb{Z}$, então $a^p \equiv a \mod p$.

Proposição 2.1.11 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a + c \equiv b + c \mod m \Leftrightarrow a \equiv b \mod m$.*

Dem.

($\Leftarrow$) Se $a \equiv b \mod m$, segue-se imediatamente da proposição 2.1.6 que $a+c \equiv b+c \mod m$ já que $c \equiv c \mod m$.

($\Rightarrow$) Se $a + c \equiv b + c \mod m$, então $m|b + c - (a + c)$, o que implica que $m|b - a$ e, consequentemente $a \equiv b \mod m$. ■

Proposição 2.1.12 *Sejam $a, b, c, m \in \mathbb{Z}$, com $c \neq 0$ e $m > 1$. Seja $d = mdc\,(c, m)$. Temos que $ac \equiv bc \mod m \Leftrightarrow a \equiv b \mod \frac{m}{d}$.*

Dem.

Observemos que $\dfrac{m}{d}$ e $\dfrac{c}{d}$ são **coprimos** [3] já que $d = mdc\,(c, m)$ logo, temos que

$$\begin{aligned} ac \equiv bc \mod m &\Leftrightarrow m|\,(b-a)\,c \\ &\Leftrightarrow \tfrac{m}{d}|(b-a)\tfrac{c}{d} \\ &\Leftrightarrow \tfrac{m}{d}|\,(b-a) \\ &\Leftrightarrow a \equiv b \mod \tfrac{m}{d} \end{aligned}$$

■

Um caso particular da proposição acima é quando $mdc(c, m) = 1$ daí, é fácil observar que $ac \equiv bc \mod m \Leftrightarrow a \equiv b \mod m$.

Proposição 2.1.13 *Sejam $a, b, m \in \mathbb{Z}$ com $m > 1$ e $mdc(b, m) = 1$. Se $a_1, a_2, ..., a_m$ é um* ***sistema completo de resíduos módulo m*** [4]*, então $a + ba_1, a + ba_2, ..., a + ba_m$ também é um sistema completo de resíduos módulo m.*

[3] Números coprimos são números primos entre si.

[4] sistema completo de resíduos módulo m é todo conjunto de números inteiros cujos restos pela divisão por m são os números $0, 1, ..., m-1$, sem repetições e numa ordem qualquer.

Dem.

Observemos que pela proposição acima se $mdc(b, m) = 1$ então, sabemos que

$$ab \equiv cb \mod m \Leftrightarrow a \equiv c \mod m.$$

Seja $i, j = 0, 1, ..., m-1$. Temos que

$$\begin{aligned} a + ba_i \equiv a + ba_j \mod m &\Leftrightarrow ba_i \equiv ba_j \mod m \\ &\Leftrightarrow a_i \equiv a_j \mod m \\ &\Leftrightarrow i = j \end{aligned}$$

já que $mdc(b, m) = 1$

Com isso, podemos afirmar que $a + ba_1, a + ba_2, ..., a + ba_m$ são, dois a dois, não congruentes módulo m e portanto, formam um sistema completo de resíduos módulo m.

■

Proposição 2.1.14 *Sejam $a, b \in \mathbb{Z}$. Se $m, n, m_1, m_2, ..., m_r$ são inteiros maiores do que 1, temos que*

1. *se $a \equiv b \mod m$ e $n|m$, então $a \equiv b \mod n$;*
2. *$a \equiv b \mod m_i$, para todo $i = 1, 2, ..., r \Longleftrightarrow a \equiv b \mod mmc(m_1, ..., m_r)$;*
3. *se $a \equiv b \mod m$, então $mdc(a, m) = mdc(b, m)$.*

Dem.

1. Observemos que se $a \equiv b \mod m$ temos por definição que $m|b-a$ mas, pelo fato de $n|m$ temos que $n|b-a$ logo, $a \equiv b \mod n$ pela definição.

2. Se $a \equiv b \mod m_i$ onde, $i = 1, 2, ..., r$, então pela definição, podemos afirmar que $m_i|b-a$ para todo i. Sendo $b-a$ um múltiplo de cada m_i, segue que $mmc(m_1, ..., m_r)\,|b-a$, o que prova que $a \equiv b \mod mmc(m_1, ..., m_r)$.

3. Se $a \equiv b \mod m$, então pela definição, $m|b-a$ logo, podemos afirmar que existe um $t \in \mathbb{Z}$ tal que $b-a = mt$, e assim, $b = a + mt$. Podemos afirmar então, pelo **lema de Euclides** [5], que

$$mdc(a, m) = mdc(a + tm, m) = mdc(b, m).$$

■

[5] Lema de Euclides: Sejam $a, b, n \in \mathbb{Z}$. Se existe $mdc(a, b-na)$, então $mdc(a, b)$ existe e $mdc(a, b) = mdc(a, b-na)$.

2.2 Congruências Lineares

Congruências Lineares são congruências do tipo:

$$aX \equiv b \mod m, \text{ onde } a, b, m \in \mathbb{Z},\ m > 1$$

Este estudo é impotante para um melhor entendimento da Aritmética das Classes Residuais para isso, necessitaremos de um importante teorema.

Teorema 2.2.1 *Dados $a, b, m \in \mathbb{Z}$, com $m > 1$ a congruência*

$$aX \equiv b \mod m$$

possui solução se, e somente se, $mdc(a, m)|b$.

Dem.

($\Rightarrow$) Suponhamos que x seja a solução da congruência $aX \equiv b \mod m$ logo, pela definição de congruência, temos que $m|ax - b$ digamos que o resultado dessa divisão seja y temos portanto que $ax - b = my$ ou ainda $ax - my = b$ logo, a equação $ax - my = b$ é uma **equação diofantina**[6] que admite como solução (x, y) logo, isso implica diretamente que $mdc(a, m)|b$.

($\Leftarrow$) Da mesma maneira, se temos que $mdc(a, m)|b$ podemos afirmar que $aX - mY = b$ admite solução que aqui, chamaremos de (x, y) logo, $ax - my = b$ ou ainda, $ax = b + my$ onde podemos afirmar que x é solução da congruência $ax \equiv b \mod m$. ∎

2.3 Aritmética das Classes Residuais

Definimos o conjunto $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$ das classes residuais módulo m, da seguinte forma:

- $\overline{0}$: é o conjunto de todos os inteiros tais que quando divisíveis por m deixam resto 0. Ou seja:

$$\overline{0} = \{x \in \mathbb{Z}; x \equiv 0 \mod m\}.$$

- $\overline{1}$: é o conjunto de todos os inteiros tais que quando divisíveis por m deixam resto 1. Ou seja:

$$\overline{1} = \{x \in \mathbb{Z}; x \equiv 1 \mod m\}.$$

...

- $\overline{k}$: é o conjunto de todos os inteiros tais que quando divisíveis por m deixam resto k. Ou seja:

[6] Equações Diofantinas são equações da forma $ax + by = c$ com $a, b, c \in \mathbb{Z}$, leva esse nome em homenagem a Diofanto de Alexandria que viveu por volta de 300 DC. Esta equação $ax + by = c$ admite solução inteira se, e somente se $(a, m)|b$.

$$\overline{k} = \{x \in \mathbb{Z}; x \equiv k \mod m\}.$$

Utilizar a aritmética das classes Residuais, é como repartir o conjunto $\mathbb{Z}$ em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divisíveis por m.

É importante observar que paramos em $\overline{m-1}$ já que temos $\overline{m} = \overline{0}$; $\overline{m+1} = \overline{1}$, e assim por diante. Vejamos um exemplo de como funciona as classes residuais.

Exemplo 2.3.1 *Seja $m = 4$, então temos:*

$$\overline{0} = \{4x; x \in \mathbb{Z}\}$$
$$\overline{1} = \{4x+1; x \in \mathbb{Z}\}$$
$$\overline{2} = \{4x+2; x \in \mathbb{Z}\}$$
$$\overline{3} = \{4x+3; x \in \mathbb{Z}\}$$

Deste modo, temos que $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

Propriedade 2.3.2 *Vejamos algumas propriedades das classes residuais:*

1. *$\overline{a} = \overline{b}$ se e somente se $a \equiv b \mod m$;*
2. *Se $\overline{a} \cap \overline{b} \neq \emptyset$, então $\overline{a} = \overline{b}$;*
3. *$\bigcup_{a \in \mathbb{N}} \overline{a} = \mathbb{Z}$.*

A demostração da propriedade é consequência direta da definição de classes residuais.

Corolário 2.3.3 *Existem exatamente m classes residuais módulo m distintas, a saber, $\overline{0}, \overline{1}, ..., \overline{m-1}$.*

Em $\mathbb{Z}_m$ definimos as seguintes operações:

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a}.\overline{b} = \overline{a.b}$$

Podemos fazer tais afirmações já que:

Se $a \equiv a' \mod m$ e $b \equiv b' \mod m$, então $\overline{a+b} = \overline{a'+b'}$ e $\overline{a.b} = \overline{a'.b'}$ pois, podemos transformar a congruência $a \equiv b \mod m$ na igualdade $\overline{a} = \overline{b}$.

A operação da adição possui quatro propriedades fundamentais.

1. **Associatividade:** $\left(\overline{a} + \overline{b}\right) + \overline{c} = \overline{a} + \left(\overline{b} + \overline{c}\right)$ para todo $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$;
2. **Comutatividade:** $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ para todo $\overline{a}, \overline{b} \in \mathbb{Z}_m$;
3. **Existência de elemento neutro:** $\overline{a} + \overline{0} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$;

4. **Existência de simétrico:** para todo $\overline{a} \in \mathbb{Z}_m$, existe $(\overline{m-a}) \in \mathbb{Z}_m$ tal que $\overline{a} + \overline{m-a} = \overline{0}$.

A operação da multiplicação possui quatro propriedades fundamentais.

1. **Associatividade:** $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$ para todo $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$;;
2. **Comutatividade:** $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ para todo $\overline{a}, \overline{b} \in \mathbb{Z}_m$;;
3. **Existência de unidade:** $\overline{a} \cdot \overline{1} = \overline{a}$, para todo $\overline{a} \in \mathbb{Z}_m$;
4. **Distributividade:** $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$, para todo $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$;.

Um conjunto qualquer munido das operações de adição e multiplicação acima é chamado de **anel** portanto, $\mathbb{Z}_m$ é chamado de **anel das classes residuais módulo m.**

Um elemento $\overline{a} \in \mathbb{Z}_m$ será chamado de **invertível**, quando existir um $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}.\overline{b} = \overline{1}$ assim, chamaremos $\overline{b}$ o inverso de $\overline{a}$.

Exemplo 2.3.4 *As tabelas de adição e multiplicação em* $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ *são*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Exemplo 2.3.5 *As tabelas de adição e multiplicação de* $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ *são*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Exemplo 2.3.6 *As tabelas de adição e multiplicação de* $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ *são*

Observemos que para $\mathbb{Z}_3$ e $\mathbb{Z}_5$ todos os elementos distintos de $\overline{0}$ é invertível pois dado um $\overline{a}$ existe um $\overline{b}$ tal que $\overline{a}.\overline{b} = \overline{1}$ mas, isso não ocorre em $\mathbb{Z}_4$ já que $\overline{0}$ não é invertível.

Um anel onde todo elemento não nulo possui um inverso multiplicativo é chamado de **corpo**. Observemos nos exemplos acima que $\mathbb{Z}_2$ e $\mathbb{Z}_5$ são corpos já $\mathbb{Z}_4$ não é um corpo.

Proposição 2.3.7 $\overline{a} \in \mathbb{Z}_m$ *é invertível se, e somente se,* $mdc\,(a, m) = 1$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\bullet$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Dem.

($\Rightarrow$)

Temos que $\overline{a}$ é invertível logo, existe um $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}.\overline{b} = \overline{1}$ por definição. Pelas propriedades fudamentais, temos que $\overline{a}.\overline{b} = \overline{a.b}$ assim $\overline{a.b} = \overline{1}$ o que nos fornece que $a.b \equiv 1 \mod m$. Desta forma, existe um $t \in \mathbb{Z}$ tal que $a.b - 1 = t.m$ fornecendo $a.b - t.m = 1$ e, consequentemente, $mdc\,(a, m) = 1$

($\Leftarrow$)

Temos que $mdc\,(a, m) = 1$ logo, existem b e t inteiros tais que $a.b + t.m = 1$ desta forma, $\overline{a.b + m.t} = \overline{1}$ mas, $\overline{a.b + m.t} = \overline{a.b} + \overline{m.t}$ pelo fato de $\overline{m.t}$ ser múltiplo de m, temos que $\overline{m.t} = 0$, logo $\overline{a}.\overline{b} + \overline{0} = \overline{a}.\overline{b}$. Assim, $\overline{a}.\overline{b} = \overline{1}$. Desta forma, $\overline{a}$ é invertível.

■

Corolário 2.3.8 *$\mathbb{Z}_m$ é um corpo se, e somente se , m é primo.*

Dem.

($\Rightarrow$)

Suponhamos por absurdo que $\mathbb{Z}_m$ é um corpo e m não é primo. Pelo fato de m não ser primo, podemos escreve-lo da seguinte forma $m = m_1.m_2$ supondo $1 < m_1 < m_2 < m$. Logo, $\overline{0} = \overline{m} = \overline{m_1}.\overline{m_2}$ mas, $\overline{m_1} \neq 0$ e $\overline{m_2} = 0$, condradição.

($\Leftarrow$)

Suponhamos agora que m é primo. Sendo $i = 1, 2, ..., m - 1$ temos que $mdc\,(i, m) = 1$, pela proposição 2.3.7, temos que $\overline{1}, \overline{2}, ..., \overline{m - 1}$ são invertíveis. Logo, $\mathbb{Z}_m$ é um corpo.

■

Capítulo 3

Introdução à Criptografia

Neste capítulo apresentaremos alguns métodos de codificação de mensagens, uma técnica milenar que vem se aprimorando a cada dia, dando suporte para evoluções tecnológicas muito utilizadas nos dias atuais como podemos verificar preferencialmente em [8], [3] e [7]. Vejamos alguns exemplos:

3.1 Cifra de Deslocamento

A cifra de deslocamento é a cifra na qual se faz um deslocamento do alfabeto, levando cada letra original à outra letra correspondente. Essa letra correspondente será a cifra utilizada para codificar um texto.

A matemática por trás da cifra de deslocamento é dada da seguinte forma:

Primeiramente, considere-se a tabela de substituição abaixo:

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

Assim, para codificar uma letra x do alfabeto, basta fazer uma translação de n letras do alfabeto, isto é,

$$E_n(x) \equiv (x + n) \mod 26$$

onde $E_n(x)$ corresponde à letra codificada correspondente à letra x.

Exemplo: Para $n = 2$ tem-se que

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$E_2(x)$	C	D	E	F	G	H	I	J	K	L	M	N	O
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$E_2(x)$	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Logo, a frase:

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado,"

quando codificada se torna:

"OCKU XCNG C NCITKOC FC FGTTQVC, FQ SWG C XGTIQPJC FG PCQ VGT NWVCFQ."

Para decodificar uma mensagem cifrada pela cifra de deslocamento, basta tomar uma letra y da mensagem cifrada e fazer a translação de n letras contrárias a da codificação, isto é,

$$D_n(y) \equiv (y - n) \mod 26$$

onde, $D_n(y)$ corresponde à letra original da letra cifrada y.

Assim, tem-se

$$D_n(E_n(x)) \equiv x \mod 26$$

Exemplo: No caso $n = 2$

x	A	B	C	D	E	F	G	H	I	J	K	L	M	$D_2(y)$
$E_2(x)$	C	D	E	F	G	H	I	J	K	L	M	N	O	y
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	$D_2(y)$
$E_2(x)$	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	y

e assim, obtem -se a frase original:

y	O	C	K	U	X	C	N	G	C	N	C	...
D_n	M	A	I	S	V	A	L	E	A	L	A	...

Na cifragem, as letras eram juntadas em um bloco único, dificultando ainda mais a decodificação da mensagem.

Note-se que as cifras de deslocamento são muito inseguras, pois com uma quantidade normalmente pequena de testes, é possível descobrir a frase original.

3.1.1 A Cifra de César

A cifra de César é um caso particular da cifra de deslocamento, ela consiste em fazer um deslocamento do alfabeto de três letras ou seja, cada letra do alfabeto original é substituida por uma letra que se encontra três unidade à sua frente. Neste caso:

$$E_3(x) \equiv (x+3) \mod 26$$

$$D_3(x) \equiv (x-3) \mod 26$$

Observe-se o exemplo da frase:

"A doçura no falar aumenta o saber."

Fazendo o deslocamento do alfabeto de três letras, chega-se à seguinte frase criptografada:

"D GRFXUD QR IDODU DXPHQWD R VDEHU."

Reza a lenda que a cifra de César foi muito utilizada por Júlio Cesar para se comunicar com seus generais, pois caso houvesse uma interceptação da mensagem, não seria possível descobri-la.

Figura 3.1: Modelo de cifra de César [7],

[7] figura retirada de http://clubedosgeeks.com.br/sem-categoria/cifra-de-cesar-criptografia-monoalfabetica

3.2 Cifrários por Substituição

O cifrário por substituição consiste em pegar cada letra do alfabeto original e substituir por uma letra qualquer do mesmo alfabeto.

Observe-se que a cifra de deslocamento é um caso particular da cifra de substituição. Um exemplo da cifra de substituição é dado a seguir:

Alfabeto original	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Letra correspondente	Q	W	E	R	T	Y	U	I	O	P	A	S	D

Alfabeto original	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Letra correspondente	F	G	H	J	K	L	Z	X	C	V	B	N	M

Caso se queira codificar a frase

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado."

pelo método da substituição acima, resultaria na seguinte frase codificada

"DQOL CQST Q SQUKODQ RQ RTKKGZQ RG JXT Q CTKUGFIQ RT FQG ZTK SXZQRG."

Aparentemente, esse método de codificação parece seguro, já que com a utilização do princípio de contagem é possível encontrar 26! maneiras diferentes de se efetuar tais trocas. Apesar de ser uma quantia considerável de permutações, com um número maior do que 403 setilhões de codificações distintas, esse método não é seguro.

Supondo que se queira decifrar a mensagem acima, porém não se tem a chave que faz a quebra desse código, a sua criptoanálise se dá por meio da contagem da quantidade de vezes que cada caractere aparece no texto, pois todo idioma tem um padrão de ocorrência das letras no alfabeto. Abaixo apresenta-se uma tabela com as frequências relativas das letras na Língua Portuguesa, todas representadas em porcentagem.

Letra	A	B	C	D	E	F	G
Probabilidade	14,66	1,04	3,88	4,10	12,57	1,02	1,30
Letra	H	I	J	K	L	M	N
Probabilidade	1,28	6,18	0,40	0,02	2,78	4,75	5,05
Letra	O	P	Q	R	S	T	U
Probabilidade	10,73	2,52	1,20	6,53	7,81	4,34	4,64
Letra	V	W	X	Y	Z	—	—
Probabilidade	1,70	0,01	0,21	0,01	0,47	—	—

Tabela 3.1: Tabela de frequência de letras da Língua Portuguesa.

Graficamente tem-se,

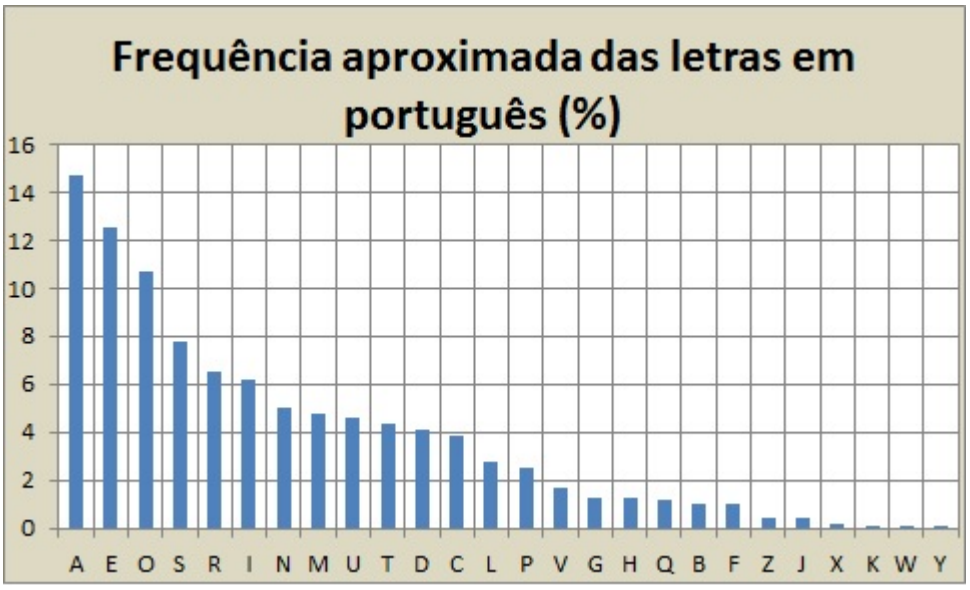


Figura 3.2: Gráfico das porcentagens de frequência das letras na Língua Portuguesa.

Ao fazer a comparação dos dados da tabela 3.1 com o texto codificado, pode-se deduzir algumas letras que estão codificadas pela quantidade de ocorrências que a mesma possui. Quanto maior o texto codificado, maior será a precisão para parâmetro de comparação entre o texto e a tabela.

Veja-se um exemplo.

Seja o texto codificado,

TD FGLLQ CORQ EGDG FQ DQZTDQZOEQ RTCTDGL LGDQK
QSTWKOQL RODOFXOK ZKOLZTMQL DXSZOHSOEQK YTSOEORQRT
T ROCOROK QDGK. FTLZQL RODTFLGTL,

ETKZQDTFZT ZGRGL WGLZQDGL RQ DQZTDQZOEQ

Abaixo, encontra-se a tabela de ocorrências de algumas letras do texto codificado.

Letra	Número de ocorrências	Letra	Número de ocorrências
Q	20	Z	10
T	16	R	10
O	16	K	7
L	14	F	6
D	13	E	6
G	11	X	2

Tabela 3.2: Frequência das letras no texto codificado

Como a frequência das letras em português segue a ordem A E O S R ... (vide tabela 3.2), muito provavelmente a letra Q deve ser a codificação da letra **a**, pois é a mais frequente. Fazendo a substituição, obtém-se a seguinte frase.

TD FGLLa CORa EGDG Fa DaZTDaZOEa RTCTDGL LGDaK
aSTWKOaL RODOFXOK ZKOLZTMaL DXSZOHSOEaK YTSOEORaRT
T ROCOROK aDGK. FTLZaL RODTFLGTL,
ETKZaDTFZT ZGRGL WGLZaDGL Ra DaZTDaZOEa.

A letra codificada é representada por minúscula para diferenciar das demais.

Agora, observe-se que a segunda letra de maior frequência é a T, que possivelmente será a codificação da letra **e**. Caso essa alteração não faça sentido no texto, deve-se substituir o T por uma outra letra com uma frequência elevada.

Verificando se T é a codificação de **e**:

eD FGLLa CORa EGDG Fa DaZeDaZOEa ReCeDGL LGDaK
aSeWKOaL RODOFXOK ZKOLZeMaL DXSZOHSOEaK YeSOEORaRe
e ROCOROK aDGK. FeLZaL RODeFLGeL,
EeKZaDeFZe ZGRGL WGLZaDGL Ra DaZeDaZOEa.

Observando-se que a primeira palavra em negrito se parece com “em”então, possivelmente, a letra D é a codificação de **m**.

Verificando se faz algum sentido.

em FGLLa CORa EGmG Fa **maZemaZOEa** ReCemGL LGmaK
aSeWKOaL ROmOFXOK ZKOLZeMaL mXSZOHSOEaK YeSOEORaRe
e ROCOROK amGK. FeLZaL ROmeFLGeL,
EeKZameFZe ZGRGL WGLZamGL Ra maZemaZOEa.

Observa-se que a palavra em negrito **maZemaZOEa** deve ser MATEMÁTICA. Se assim for, Z é **t**, O é **i** e E é **c**. Fazendo estas substituições:

em **FGLLa** CiRa cGmG Fa matemática ReCemGL LGmaK
aSeWKiaL RimiFXiK tKiLZeMaL mXSZiHSiEaK YeSiEiRaRe
e RiCiRiK amGK. FeLtaL RimeFLGeL,
ceKtameFte tGRGL WGLtamGL Ra matemática.

Observando novamente o número de ocorrências das letras, a letra L possui um alto índice de frequência então, possivelmente L será a codificação das letras **o**, **s** ou **r**.

Observando a palavra em negrito **FGLLa**, pode-se deduzir que dificilmente L será o codificador de **o** já que haveria dois **o's** juntos.

Verificando então se L codifica **s**:

em FGssa CiRa **cGmG** Fa matemática ReCemGs sGmaK
aSeWKias RimiFXiK tKisZeMas mXSZiHSiEaK YeSiEiRaRe
e RiCiRiK amGK. Festas RimeFsGes,
ceKtameFte tGRGs WGstamGs Ra matemática.

Observando-se novamente o texto, pode-se deduzir pela palavra em negrito **cGmG**, que G será o codificador de **o**, pela segunda palavra em negrito **ceKtameFte**, que K será **r** e F será **n**.

Verificando:

em nossa CiRa como na matemática ReCemos somar
aSeWrias RimiFXir trisZeMas mXSZiHSiEar YeSiEiRaRe
e RiCiRir amor. nestas **Rimensoes**,
certamente toRos Wostamos Ra matemática.

Agora, note-se que **Rimensoes** possivelmente será dimensões logo, R será o codificador de **d**.

Verificando:

em nossa Cida como na matemática deCemos somar
aSeWrias dimiFXir trisZeMas mXSZiHSiEar YeSiEidade
e diCidir amor. nestas dimensoes,
certamente todos Wostamos da matemática.

Fazendo isso até que se esgotem todas as letras, teremos o texto decodificado.

Em nossa vida, como na matemática, devemos somar
alegrias, diminuir tristezas, multiplicar felicidade
e dividir amor. Nestas dimensões,
certamente todos gostamos da matemática.

Esse método de decifragem pode ser utilizado para encontar quaisquer cifras que estejam utilizando métodos de substituições. Apesar da grande quantidade de codificações possíveis, é importante observar que esse método de cifragem não é seguro.

3.2.1 O Atbash Hebráico

O Atbash Hebráico é uma criptografia em que se troca a primeira letra pela última, a segunda pela penúltima, e assim sucessivamente ou seja,

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

Observem que à letra A corresponde a Z, B corresponde a Y, C corresponde a X, e assim sucessivamente. Caso se queira codificar a frase

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado."

obtem-se

"NZRH EZOV Z OZTINZ WZ WVIILGZ, WL JFV Z EVITLMSA WV MZL GVI OFGZWL."

Ao se conhecer o método de codificação de um determinado texto, a decodificação se torna direta, basta utilizar o processo inverso para que se conheça a frase original.

3.2.2 O Cifrário de Políbio

O cifrário de Políbio é uma técnica utilizada para alfabetos com 25 letras. Como o alfabeto da Língua Portuguesa possui 26 letras, será retirada a letra "**w**" e, quando necessário, será usado o "**k**" no seu lugar. Essa técnica consiste em distribuir as letras do alfabeto numa matriz quadrada de ordem 5 (5 linhas e 5 colunas).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Figura 3.3: Cifrário de Políbio

Cada letra deve ser substituida por sua linha correspondente e sua coluna nessa ordem. Por exemplo, a letra **r** se transforma em 43 o que corresponde à quarta linha e terceira coluna, já o **h** se transforma em 23.

Seja um trecho da frase:

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado."

Criptografando apenas o início:

"Mais vale a lágrima da derrota"

Observe-se que M ocupa a terceira linha e terceira coluna, logo, será substituido por 33; o **a** ocupa a primeira linha e primeira coluna, logo, equivale a 11 e assim sucessivamente.

Ao criptografá-la encontra-se:

"33 11 24 44 52 11 32 15 11 32 11 22 43 24 33 11 14 11 14 11 14 15 44 44 35 45 11"

Aqui, novamente, coloca-se os espaços para melhor compreensão.

A cifra de Políbio possui inicialmente duas deficiências. A primeira é que ela dobra o tamanho do texto original já que cada letra é substituida por uma dupla de números. A segunda é que aparentemente é fácil de "quebrar"sua codificação já que basta distibuir o alfabeto em uma matriz 5×5 e ir substituindo as duplas de números por suas linhas e colunas correspondentes. Para minimizar a quebra dessa cifra, deve-se proceder da seguinte forma:

Inicialmente escolhe-se uma palavra chave que será colocada nas primeiras posições da matriz. Caso essa palavra possua letras repetidas, mantem somente a de primeira ocorrência; para as demais posições

não ocupadas, segue-se o alfabeto na sua ordem tomando apenas o cuidado para não repetir as letras já utilizadas. Será utilizada a palavra chave "NATALIA"para exemplificar o processo.

	1	2	3	4	5
1	N	A	T	L	I
2	B	C	D	E	F
3	G	H	J	K	M
4	O	P	Q	R	S
5	U	V	X	Y	Z

Figura 3.4: Cifrário de Políbio com palavra chave

Ao fazer esse ajuste, pode-se observar que as letras não ficam na ordem em que aparecem no alfabeto, dificultando consideravelmente a quebra da mensagem. Ao receber o texto codificado, o receptor deve ter conhecimento da palavra chave e em posse dela, utiliza o mesmo processo para decodifica-la.

3.2.3 Cifra de Hill

Esta cifra inventada pelo americano Lester Hill, em 1929, contribuiu em larga escala para tornar a criptografia mais algébrica. Ela consiste em, inicialmente, tomar uma matriz quadradra invertível $n \times n$ módulo 26 da forma

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

em que cada entrada a_{ij} são números inteiros em $\mathbb{Z}_{26}$. Essa é a chave do processo. Para criptografar uma mensagem utilizando a cifra de Hill, deve-se primeiramente quebrar a mensagem em partes contendo **n** caracteres, sendo **n** a ordem da matriz dada. Seja X o texto a ser criptografado e

$$x_1x_2x_3...x_n$$

cada letra do bloco partido em **n** caracteres. Para cada letra do alfateto, atribui-se um valor pré-estabelecido.

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

Após a troca das letras pelos seus devidos valores, efetua-se o produto matricial

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

onde as operações são efetuadas módulo 26, para obter-se o bloco criptografado

$$y_1 y_2 y_3 ... y_n$$

Se o último bloco de letras do texto original não possuir exatamente **n** letras, ele deve ser completado com letras que não alterem o sentido original da frase. Após esse processo, troca-se os valores $y_1 y_2 y_3 ... y_n$ que nesse momento estão em formato numérico, por suas respectivas letras. Utilizando-se esse método até se esgotarem os blocos, o texto estará codificado.

Verificando um exemplo:

Seja uma matriz M da forma

$$M = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

Supondo querer-se criptografar a palavra **amor**. Fazendo a substituição letra a letra pelos seus respectivos valores, tem-se que **amor = (0, 12, 14, 17)**. Vamos utilizar a técnica de Hill para fazer a codificação. Utilizando M como chave e efetuando as operações módulo 26 tem-se.

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 96 \\ 84 \end{pmatrix} = \begin{pmatrix} 18 \\ 6 \end{pmatrix} = \begin{pmatrix} s \\ g \end{pmatrix}$$

$$\begin{pmatrix} y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix}$$

$$\begin{pmatrix} y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 290 \\ 161 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix} = \begin{pmatrix} e \\ f \end{pmatrix}$$

A mensagem cifrada é então **sgef**.

Para decodificar a mensagem, é necessário encontrar a matriz inversa da chave M. Uma matriz quadrada A com elementos em $\mathbb{Z}_{26}$ é invertível em $\mathbb{Z}_{26}$ se existir outra matriz B com elementos em $\mathbb{Z}_{26}$ tal que $AB = I$ onde I é a matriz identidade de ordem n em $\mathbb{Z}_{26}$.

Essa necessidade se dá pelo fato de que

$$\begin{pmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{n1} \end{pmatrix} = M. \begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix}$$

$$M^{-1} \begin{pmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{n1} \end{pmatrix} = M^{-1}M. \begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix}$$

assim,

$$\begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix} = M^{-1} \begin{pmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{n1} \end{pmatrix},$$

onde $y_1y_2y_3...y_n$ corresponde ao texto codificado inicialmente e $x_1x_2x_3...x_n$ corresponde ao texto original.

A inversa da matriz

$$M = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

em $\mathbb{Z}_{26}$ é dado por

$$M^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

Veja-se o método para decodificar a mensagem cifrada.

Seja a mensagem codificada **sgef**. Observem que **sgef = (18, 6, 4, 5)** assim, para encontrar os valores originais de $x_1x_2x_3...x_n$ tem-se que

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 18 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 234 \\ 480 \end{pmatrix} = \begin{pmatrix} 0 \\ 12 \end{pmatrix} = \begin{pmatrix} a \\ m \end{pmatrix},$$

assim como,

$$\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 4 \\ 5 \end{pmatrix}$$

$$\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 118 \\ 147 \end{pmatrix} = \begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} o \\ r \end{pmatrix},$$

O que fornece a decodificação da mensagem **sgef** para a mensagem original **amor**.

3.2.4 Cifra Afim

A cifra afim consiste, inicialmente, em fazer uma substituição das letras do alfabeto por números inteiros entre 0 e 25, seguindo a tabela

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

e depois tomar a seguinte função de criptografar.

$$y_i = c(x_i) \equiv (ax_i + b) \mod 26,$$

Onde **a** e **b** são números em $\mathbb{Z}_{26}$, x_i é a i-ésima letra do alfabeto original, y_i é a i-ésima letra do texto cifrado e $c(x_i)$ corresponde à codificação da letra x_i.

É importante observar que a função acima deve ser injetiva em $\mathbb{Z}_{26}$, pois caso contrário, para duas ou mais letras do alfabeto original ter-se-ia que as elas corresponderiam a uma mesma letra quando cifrada.

Verificando um exemplo para a função $y_i \equiv (13x_i + 3) \mod 26$.

- Para a letra A temos que $x_i = 0$ logo:

  $y_i \equiv (13.0 + 3) \mod 26 \rightarrow y_i \equiv 3 \mod 26 \rightarrow y_i = D$

- Para a letra B temos que $x_i = 1$ logo:

  $y_i \equiv (13.1 + 3) \mod 26 \rightarrow y_i \equiv 16 \mod 26 \rightarrow y_i = Q$

- Para a letra C temos que $x_i = 2$ logo:

  $y_i \equiv (13.2 + 3) \mod 26 \rightarrow y_i \equiv 29 \mod 26 \rightarrow y_i \equiv 3 \mod 26 \rightarrow y_i = D$

Observe-se que essa função não é injetiva, logo não serve para criptografar uma mensagem, pois leva os números pares 0, 2, 4, ... em $\mathbb{Z}_{26}$ no 3 que corresponde a D e os números ímpares em $\mathbb{Z}_{26}$ no 16 que corresponde a Q assim, o texto cifrado só teria duas letras o D e o Q.

Para que a função $y_i = ax_i + b$ seja injetiva em $\mathbb{Z}_{26}$ devemos ter que a e 26 sejam primos entre si. Quando isso ocorre, tem-se que a função

$$y_i = c(x_i) \equiv (ax_i + b) \mod 26,$$

serve para codificar o texto original, e a função

$$x_i = d(y_i) \equiv a^{-1}(y_i - b) \mod 26$$

serve para decodificar o texto cifrado, em que a^{-1} indica o inverso módulo 26 de a. Vejam um exemplo. Considerando-se o codificador:

$$y_i = c(x_i) \equiv (7x_i + 1) \mod 26,$$

Observando que 7 e 26 são primos entre si, a função é injetiva módulo 26.

- Para a letra A temos que $x_i = 0$ logo:

  $y_i \equiv (7.0 + 1) \mod 26 \rightarrow y_i \equiv 1 \mod 26 \rightarrow y_i = B$

- Para a letra B temos que $x_i = 1$ logo:

  $y_i \equiv (7.1 + 1) \mod 26 \rightarrow y_i \equiv 8 \mod 26 \rightarrow y_i = I$

- Para a letra C temos que $x_i = 2$ logo:

  $y_i \equiv (7.2 + 1) \mod 26 \rightarrow y_i \equiv 15 \mod 26 \rightarrow y_i = P$

-
-
-

A tabela seguinte, fornece as devidas codificações:

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

Isso faz com que a letra A seja representada pela letra B quando codificada, a letra B pela letra I, a letra C pela letra P e assim sucessivamente.

Por exemplo, a mensagem:

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado."

fica assim codificada:

"HBFX SBAD B ABRQFHB WB WDQQVEB, WV JLD B SDQRVOYB WD OBV EDQ ALEBWV."

Para decifrar a mensagem já codificada, inicialmente deve-se encontrar o inverso de 7 módulo 26 que é 15 já que, $15.7 \equiv 1 \mod 26$. A função que serve como decodificador da mensagem é dada por:

$$x_i = d(y_i) \equiv a^{-1}(y_i - b) \mod 26,$$

logo,

$$x_i = d(y_i) \equiv 15(y_i - 1) \mod 26,$$

que equivale à:

$$x_i = d(y_i) \equiv (15y_i + 11) \mod 26$$

Ou seja, quando o texto está codificado, a letra P correspondente a $y_i = 15$ representa

$$x_i = d(15) \equiv (15.15 + 11) \mod 26$$
$$x_i = d(15) \equiv (236) \mod 26$$
$$x_i = d(15) \equiv 2 \mod 26$$

logo, P corresponde a $x_i = 2$ que equivale a C quando codificado. Fazendo esse processo para todas as letras do alfabeto codificadas do texto, temos que a mensagem estará decodificada.

3.3 Cifrário Bifendido de Delastelle

O Cifrário Bifendido de Delastelle utiliza a mesma técnica de matriz quadrada que o cifrário de Políbio.

Para utilizarmos esse método, deve-se escrever a frase em forma de linhas com n caracteres cada, e abaixo de cada letra, coloca-se o número de sua linha; abaixo do número da linha, o número correspondente à sua coluna. Após esse processo, copia-se todos os números linha por linha, ordenadamente, de um mesmo bloco. Feita essa etapa, agrupam-se todos os números formando uma única frase. Em posse da frase, forma-se duplas entre os números ordenadamente onde, posteriormente, deve-se substitui-los pela letra correspondente à matriz.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Figura 3.5: Cifrário bifendido de Delastelle

Observem a frase:

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado".

na qual será cifrado:

"Mais vale a lágrima"

Isso corresponde a quebrar a frase em blocos contendo 16 caracteres cada.

Inicialmente colocam-se as letras na forma de tabela, e abaixo deve-se escrever sua respectiva linha e coluna.

M	**A**	**I**	**S**	**V**	**A**	**L**	**E**	**A**	**L**	**A**	**G**	**R**	**I**	**M**	**A**	**Frase original**
3	1	2	4	5	1	3	1	1	3	1	2	4	2	3	1	**Número da linha**
3	1	4	4	2	1	2	5	1	2	1	2	3	4	3	1	**Número da coluna**

Observe que a letra M ocupa a terceira linha e terceira coluna, a letra A ocupa a primeira linha e primeira coluna, a letra I ocupa a segunda linha e quarta coluna, e assim sucessivamente. Copiando a sequência linha por linha encontra-se:

3124513113124231 3144212512123431

Fazendo a separação dos números aos pares obtem-se:

31/24/51/31/13/12/42/31/31/44/21/25/12/12/34/31

Agora, deve-se procurar na matriz, as letras correspondentes a cada par de números acima. Fazendo as devidas substituições, temos por exemplo, que o elemento 31 corresponde à letra que está na terceira linha e primeira coluna, K; 24 corresponde à letra que se encontra na segunda linha e quarta coluna, I, e assim sucessivamente. Verificando como fica a frase cifrada:

"KIUKCBQKKSFJBBNK"

Agora, para descriptografar o texto codificado, deve-se utilizar o seguinte processo.

Inicialmente, coloca-se a frase codificada na forma de tabela, e abaixo deve-se escrever sua respectiva linha e coluna.

K	**I**	**U**	**K**	**C**	**B**	**Q**	**K**	**K**	**S**	**F**	**J**	**B**	**B**	**N**	**K**	**Frase codificada**
3	2	5	3	1	1	4	3	3	4	2	2	1	1	3	3	**Número da linha**
1	4	1	1	3	2	2	1	1	4	1	5	2	2	4	1	**Número da coluna**

Após esse processo, copia-se os números de cima para baixo, da esquerda para a direita obtendo:

3124513113124231 3144212512123431

Feito isso, dividi-se o bloco em duas partes iguais e coloca-se um abaixo do outro formando duas linhas da seguinte forma:

3	1	2	4	5	1	3	1	1	3	1	2	4	2	3	1	**Primeiro bloco**
3	1	4	4	2	1	2	5	1	2	1	2	3	4	3	1	**Segundo bloco**

O primeiro bloco será a linha correspondente a cada letra da frase decodificada, e o segundo bloco será a coluna correspondente a cada letra da frase decodificada. Fazendo as devidas substituições tem-se:

3	1	2	4	5	1	3	1	1	3	1	2	4	2	3	1	**Número da linha**
3	1	4	4	2	1	2	5	1	2	1	2	3	4	3	1	**Número da coluna**
M	**A**	**I**	**S**	**V**	**A**	**L**	**E**	**A**	**L**	**A**	**G**	**R**	**I**	**M**	**A**	**Frase original**

Que nos fornece o trecho **"Mais vale a lágrima"** como era esperado.

3.4 Transposição Colunar

A transposição colunar consiste em colocar a frase original em uma matriz $n \times m$ escrevendo da esquerda para a direita no formato padrão. Após a divisão da matriz em **n** blocos, troca-se as colunas por uma ordem pré-estabelecida. Essa ordem pré-estabelecida corresponde à chave da decodificação.

Por exemplo, considere a frase

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado."

distribuída em uma matriz formada por **m** colunas.

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
m	a	i	s	v	a	l	e	a
l	a	g	r	i	m	a	d	a
d	e	r	r	o	t	a	d	o
q	u	e	a	v	e	r	g	o
n	h	a	d	e	n	a	o	t
e	r	l	u	t	a	d	o	m

Em seguida, fazendo-se uma transposição das colunas pré-estabelecidas na seguinte ordem 2 3 1 4 8 9 7 6 5, chega-se à seguinte matriz

2	**3**	**1**	**4**	**8**	**9**	**7**	**6**	**5**
a	i	m	s	e	a	l	a	v
a	g	l	r	d	a	a	m	i
e	r	d	r	d	o	a	t	o
u	e	q	a	g	o	r	e	v
h	a	n	d	o	t	a	n	e
r	l	e	u	o	m	d	a	t

Copiando-se linha por linha, temos que o texto codificado será:

"AIMSEALAV AGLRDAAMI ERDRDOATO UEQAGOREV HANDOTANE RLEUOMDAT".

Observem que a chave empregada para cifrar a mensagem é a mesma para decifrá-la. Nesse caso, conhecendo-se a sequência 231489765, basta copiar as letras do texto codificado na ordem em que a sequência

sugere. A primeira letra do texto codificado será a segunda do texto original, a segunda letra do texto codificado será a terceira do texto original, a terceira letra do texto codificado será a primeira do texto original, e assim por diante. Fazendo esse processo até que se esgote todo o texto, tem-se que a mensagem estará decifrada.

3.4.1 A Cítala Espartana

Era um método muito utilizado pelos éforos espartanos para envio de mensagens secretas. Ela consiste em enrolar, em espiral, uma tira de papiro ou de pergaminho em torno de um cilindro qualquer. A mensagem era escrita de cima para baixo na mesma vertical. Ao desenrrolar o pergaminho, a mensagem formava um "cinto"com caracteres todos misturados e sem sentido. A mensagem só era decodificada com um cilindro de mesmo raio. O Bastão de Licurgo, que data do século V a.C., é um exemplo desse processo. O remetente escrevia a mensagem ao longo do bastão e depois desenrolava a tira de couro a qual passava a conter apenas um monte de letras sem sentido algum.

Figura 3.6: Bastão de Licurgo [8]

Muito utilizado no século V a.c., a cítala espartana basicamente consiste em tomar uma matriz $n \times m$ onde **n** representa à quantidade de caracteres correspondentes a uma mesma vertical do cilindro ou seja, a quantidade de linhas que a matriz deve possuir. A frase a ser codificada é escrita de cima para baixo a partir da primeira coluna. Ao escrever **n** caracteres, a quantidade de linhas se esgotará e, então, deve-se seguir o mesmo processo, escrevendo agora as letras nas demais colunas até que se esgotem todas as letras da frase a ser codificada. A chave para decifrar o segredo é encontrar a quantidade de colunas que possui a matriz já que essa fornecerá o tamanho de cada bloco em que deve-se separar a frase codificada.

Exemplo: a frase

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado."

é criptografada pela cítala espartana da seguinte forma: toma-se uma matriz com $n = 6$ linhas. A quantidade de colunas **m** se dará ao final da trascrição da mensagem. Nesse caso, $m = 9$.

[8] figura retirada de http://pt.wikipedia.org/wiki/Cítalamediaviewer/File:Skytale.png

$$\begin{pmatrix} M & L & R & D & A & A & N & A & U \\ A & E & I & E & D & V & H & O & T \\ I & A & M & R & O & E & A & T & A \\ S & L & A & R & Q & R & D & E & D \\ V & A & D & O & U & G & E & R & O \\ A & G & A & T & E & O & N & L & U \end{pmatrix}$$

Observem que foi adicionada uma letra para completar a matriz que não mudará o sentido da frase.

Dividindo-se a matriz em blocos, tem-se:

"MLRDAANAU AEIEDVHOT IAMROEATA SLARQRDED VADOUGERO AGATEONLU."

Os espaços foram colocados somente para melhor visualização da cifra. No final, retiram-se os espaços e os acentos para dificultar a decodificação.

Para quebrar a cifra codificada, basta que se conheça a quantidade de colunas que a mesma possui. A partir desse momento, deve-se dividir a cifra em blocos cuja quantidade de letras deve ser igual à quantidade de colunas. Ao fazer isso no texto inteiro, basta colocar os blocos um abaixo do outro e copiar a mensagem de cima para baixo da esquerda para a direita. Neste momento, a mensagem estará decidificada.

3.5 Permutação

Esse método consiste em quebrar uma mensagem em blocos de n letras e depois trocá-las de acordo com uma permutação pré-definida das mesmas.

Uma maneira de fazer essa permutação de n letras, é tomando uma função bijetora.

$$f : \{1, 2, 3, ..., n\} \longrightarrow \{1, 2, 3, ..., n\}$$

Por exemplo:

Se a mensagem original for quebrada em blocos de quatro letras, pode-se, então, tomar a seguinte permutação:

$$f : \{1, 2, 3, 4\} \to \{3, 4, 2, 1\}$$

$$1 \xrightarrow{f} 3$$
$$2 \xrightarrow{f} 4$$
$$3 \xrightarrow{f} 2$$
$$4 \xrightarrow{f} 1$$

Isto é; $f(1) = 3$, $f(2) = 4$, $f(3) = 2$ e $f(4) = 1$.

Agora a primeira letra do texto a ser cifrado será substituida pela terceira letra do texto, a segunda letra será substituida pela quarta, e assim sucessivamente.

Caso a quantidade de letras do texto a ser cifrado não seja múltiplo da quantidade de letras por bloco pretendido, deve-se adicionar letras ao final do texto para que os blocos fiquem todos completos, tomando-se apenas o cuidado para que as letras adicionadas não alterem a mensagem original. Vejam o exemplo com a função acima, para criptografar a frase:

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado"

Fazendo a divisão da frase em grupos de 4 letras, tem-se:

1	2	3	4	1	2	3	4	1	2	3	4	...	**números de entrada da função**
M	**A**	**I**	**S**	**V**	**A**	**L**	**E**	**A**	**L**	**A**	**G**	...	**texto a ser cifrado**
3	4	2	1	3	4	2	1	3	4	2	1	...	**aplicação da função**
I	**S**	**A**	**M**	**L**	**E**	**A**	**V**	**A**	**G**	**L**	**A**	...	**texto cifrado**

Observem que a frase

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado."

quando cifrada fica da seguinte forma:

"ISAM LEAV AGLA MAIR DEAD OTRR OQDA AVEU GORE ADHN AONE RLET ADTU DMAO."

Aqui, colocou-se as letras **ADM** ao final do texto para que todos os blocos ficassem completos, além de colocar os espaços somente para facilitar a leitura.

É importante observar que a cifra de permutação não altera as letras originais, ela somente as trocam as mesmas de ordem.

Para fazer a **"quebra"** da frase cifrada, é necessário saber a função inversa de **f**. A função definida como:

$$f : \{1, 2, 3, 4\} \to \{3, 4, 2, 1\}$$

$$1 \xrightarrow{f} 3$$
$$2 \xrightarrow{f} 4$$
$$3 \xrightarrow{f} 2$$
$$4 \xrightarrow{f} 1$$

faz com que a primeira letra de cada grupo seja substituída pela terceira, a segunda pela quarta, e assim sucessivamente. Logo, a primeira letra do texto codificado deve ser substituida pela quarta letra, a segunda letra do texto codificado deve ser substituida pela terceira, a terceira pela primeira e a quarta pela segunda. Logo, obtem-se a seguinte estrutura:

$$f : \{1, 2, 3, 4\} \to \{3, 4, 2, 1\}$$

$$1 \overset{f^{-1}}{\leftarrow} 3$$
$$2 \overset{f^{-1}}{\leftarrow} 4$$
$$3 \overset{f^{-1}}{\leftarrow} 2$$
$$4 \overset{f^{-1}}{\leftarrow} 1$$

portanto, deve-se definir a função inversa como:

$$f^{-1} : \{1, 2, 3, 4\} \to \{4, 3, 1, 2\}$$

1	2	3	4	1	2	3	4	1	2	3	4	...	**entradas da função inversa**
I	**S**	**A**	**M**	**L**	**E**	**A**	**V**	**A**	**G**	**L**	**A**	...	**texto cifrado**
4	3	1	2	4	3	1	2	4	3	1	2	...	**aplicação da função inversa**
M	**A**	**I**	**S**	**V**	**A**	**L**	**E**	**A**	**L**	**A**	**G**	...	**texto decodificado**

É importante observar que quanto maior for o texto, mais difícil se torna sua decodificação já que funções maiores podem ser montadas dificultando-se assim, a quebra dele.

3.6 A Máscara de Matias Sandorf

Na antiguidade, os escritores usavam seus conhecimentos sobre criptografia para dar uma pitada de emoção em seus contos. Como exemplo Júlio Verne (francês, 1828-1905) descreveu, em um de seus livros, um método que ficou conhecido como “A Máscara de Matias Sandorf”.

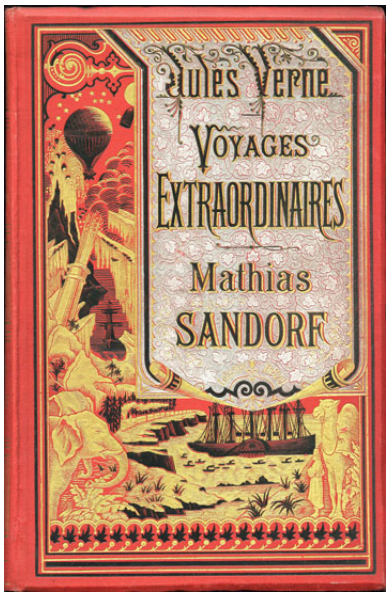


Figura 3.7: Livro de Júlio Verne [9]

A máscara de Matias Sandorf é uma técnica chamada de **esteganografia**, ou a arte de ocultar uma mensagem. Ela consiste em numa matriz quadrado 6×6, escrever a frase a ser cifrada da esquerda para a direita, até que se preencha todos os espaços. Com o auxilio de uma "máscara", que também deve ser uma matriz quadrada e de mesma ordem que a matriz em que se colocou a cifra, fazer uma grade onde apenas algumas letras do texto devem estar visíveis. Copia-se as letras visíveis da esquerda para a direita e de cima para baixo e, em seguida, gira-se a máscara 90 graus no sentido horário, fazendo o mesmo procedimento da etapa anterior. Após sucessivos processos idênticos, todas as letras da matriz serão contempladas.

É importante observar que em cada etapa devem ser copiadas $\frac{36}{4} = 9$ letras. Deve-se tomar o cuidado de se formar uma máscara onde cada letra visível em cada etapa, não fique também visível nas etapas posteriores. Como se deve fazer esse processo quatro vezes, todas as letras da matriz serão contempladas uma única vez.

Para facilitar o entendimento dessa técnica, será cifrado um pedaço da frase:

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado"

Primeiramente, escolheu-se a introdução da frase acima.

"Mais vale a lágrima da derrota, do que a vergonha."

Serão retiradas as letras "**ue**"de "**que**"e a letra "**a**"de vergonha. Esse processo é utilizado para que a quantidade de letras da frase seja compatível com a quantidade de termos da matriz. Vejam como fica a frase acima na matriz.

[9]figura retirada de http://upload.wikimedia.org/wikipedia/commons/a/ac/Sandorf$_h$*etzel.jpg*

M	A	I	S	V	A
L	E	A	L	A	G
R	I	M	A	D	A
D	E	R	R	O	T
A	D	O	Q	A	V
E	R	G	O	N	H

Figura 3.8: texto original

Logo após, escolhe-se uma máscara conveniente para a matriz acima. Essa máscara será a chave da cifra tanto para codificar quanto para decodificar.

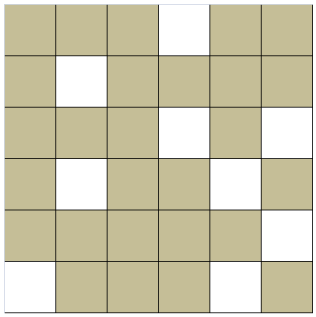


Figura 3.9: máscara de Matias Sandorf

Coloca-se a máscara sobre a matriz e copiam-se as letras da esquerda para a direita e de cima para baixo. Após esse processo, deve-se girar a máscara no sentido horário, em um ângulo de 90 graus, onde outras letras ficarão visíveis na matriz. Repete-se o processo até que comece a repetir as etapas já realizadas. Vejam como fica cada etapa da máscara de Matias Sandorf.

Figura 3.10: Cada etapa da máscara de Sandorf

Agora, copiam-se as letras visíveis após a colocação da máscara, obedecendo-se a ordem citada acima.

Na primeira etapa tem-se a seguinte ordem: $SEAAEOVEN$

Na segunda etapa: $MAARTAORO$

Na terceira etapa: $AALIDDRAG$

Na quarta e última etapa: $IVLGRMDQH$

Juntando cada uma das etapas e colocando-as na forma de frase, obtem-se a seguinte mensagem cifrada:

"SEAAEOVEN MAARTAORO AALIDDRAG IVLGRMDQH".

A pessoa que receber a mensagem codificada por esse método deve possuir a mesma máscara utilizada para cifrar a mensagem. Em posse da máscara, ela deve quebrar a mensagem em blocos de forma a preencher toda a matriz de ordem 6. Coloca-se a máscara sobre a matriz na posição combinada previamente; em seguinda, deve-se copiar as nove letras que ficaram à mostra, repetindo-se a operação até todas as letras serem contempladas.

Capítulo 4

A criptografia dentro da sala de aula

4.1 O minicurso

Diante do objetivo de utilizar a criptografia como uma ferramenta de incentivo ao estudo de Matemática, elaboramos e aplicamos um minicurso para alunos do segundo e terceiro ano do Ensino Médio de uma escola localizada na cidade de Uberlândia - Minas Gerais.

A escolha por essas séries ocorreu pelo fato de que alguns modelos de criptografia utilizam o conceito de matrizes, matéria ainda não vista pelos alunos do primeiro ano do Ensino Médio e, também, devido ao espaço físico para realização das atividades.

A proposta do minicurso foi introduzir os conceitos de divisibilidade e congruência de uma maneira lúdica, mostrando para os alunos as diferentes formas de aplicação e propriedades dessas matérias, utilizando a criptografia. Para isso, foram ministradas 10 aulas de 50 minutos cada. Ressaltamos que o minicurso não era obrigatório e foram convidados 58 alunos, com a adesão de 35 participantes.

O que foi proposto possibilitou aos alunos a percepção da aplicabilidade da matemática, via criptografia, além de despertar o interesse deles pelo conteúdo específico.

Figura 4.1: Foto da realização do minicurso.

4.1.1 Das fases do minicurso

O minicurso foi dividido em quatro etapas, sendo elas:

1. Conceitos primitivos de criptografia.
2. Introdução ao conceito de divisibilidade e de congruência.
3. A importância de divisibilidade e congruência na criptografia.
4. Codificação e decodificação de mensagens pelos métodos apresentados.

4.1.2 Primeira etapa - Conceitos primitivos de criptografia

A etapa inicial teve duração de 1 hora/aula tendo como principal objetivo mostrar aos alunos a importância da criptografia e suas diversas aplicabilidades no dia a dia em diferentes contextos históricos.

Para explanar sobre a importância da codificação de mensagens na sociedade na Era Antiga e Atual, convidamos um professor de História da escola.

Apresentamos uma abordagem histórica sobre a origem do surgimento de alguns métodos criptográficos indicando a importância dos mesmos para a sociedade. Nessa etapa podemos destacar a interdisciplinariedade

das disciplinas ao mostrar aos alunos a importância das criptografias em cada época. Foi dado maior ênfase para três aspectos históricos:

1. Na história antiga, onde Júlio Cesar não tinha o apoio do senado romano que queria "sua cabeça"de qualquer forma. As mensagens codificadas para os generais aliados eram de extrema importância.

2. Esparta, que era uma das principais polis (cidades-estado) da Grécia Antiga. Era considerada uma cidade militarizada, que vivia em guerra com os Persas e posteriormente, com Atenas. O sigilo de mensagens era essencial para táticas de combate.

3. A Segunda Guerra Mundial, onde as mensagens eram transmitidas por rádio ou telefone e portanto, fácil de ser interceptada.

Esses fatos históricos ilustram a importância da cifragem de mensagens, o que gerou um entusiasmo entre os participantes do minicurso.

4.1.3 Segunda etapa - Introdução ao conceito de divisibilidade e de congruência

A segunda etapa teve duração de 3 horas/aula, cujo objetivo foi introduzir os conceitos de divisibilidade e de congruência, mostrando suas propriedades e aplicações.

Inicialmente explicamos sobre divisibilidade, expondo os conceitos primitivos e propriedades como podemos verificar na figura 4.2. Apresentamos exemplos e realizamos exercícios, com especial destaque para o seguinte problema: Pedimos aos alunos para escreverem o quadrado dos números naturais de 1 até 20 e tentarem encontrar uma regularidade entre o quadrado desses números. A maioria dos alunos notaram que os quadrados sempre possuíam como algarismo das unidades $\{0, 1, 4, 5, 6, 9\}$. Em seguida, solicitamos que observassem que os números encontrados podiam ser escritos na forma $5k$, $5k + 1$ e $5k + 4$, o que foi feito com facilidade pelos mesmos. Após essa discussão, pedimos para que os alunos demonstrassem que todos os quadrados perfeitos são escritos dessa forma.

Notamos que a palavra demonstração soa um pouco forte para alunos do Ensino Médio, pois eles não estão familiarizados com as formalidades de uma demonstração. Afirmamos isso, pois a frase mais escutada nesse momento foi: "Mas como faço isso?"Tentamos ser o mais imparcial possível, pedindo para eles relacionarem os conteúdos que acabaram de ser vistos com o exercício proposto. Nos gerou surpresa o fato de que seis alunos, conseguiram iniciar a resolução de maneira correta sendo que dois destes concluíram o exercício corretamente.

Em busca de auxiliar os demais alunos na compreensão do exercício, pedimos que os mesmos relembrassem dos possíveis restos da divisão de um número por 5 e, posteriormente, tentassem relacionar este fato com a demonstração. Dessa forma a grande maioria dos alunos conseguiram concluir o exercício. Por fim, depois de todo esse processo, a resolução do exercício foi socializada no quadro.

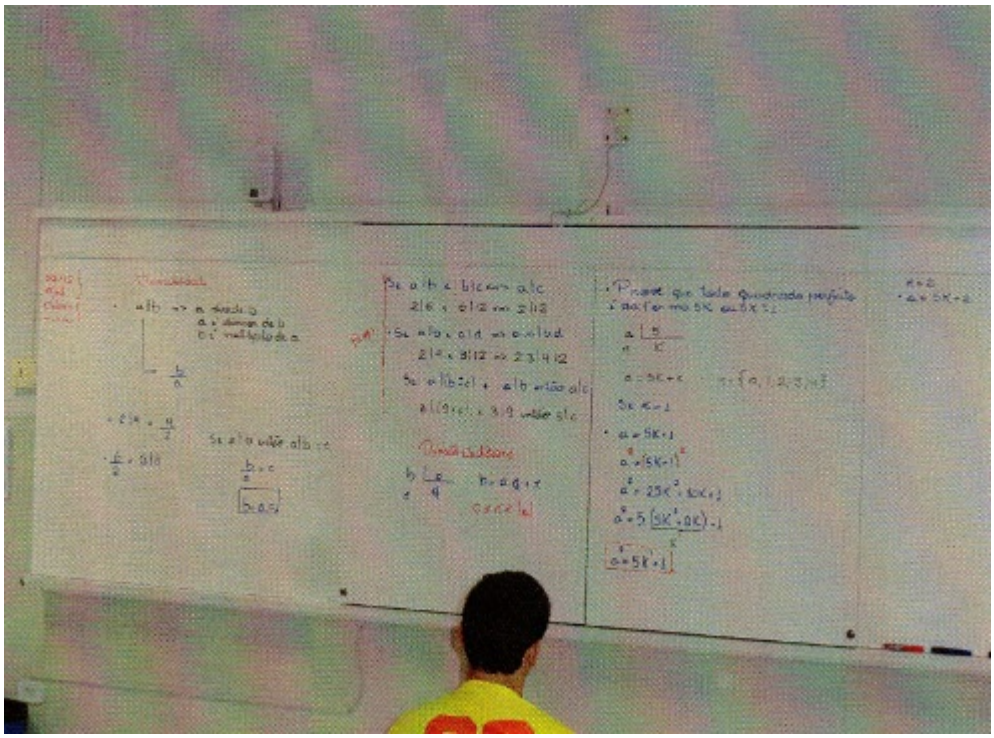


Figura 4.2: Introdução à divisibilidade.

Na segunda metade dessa etapa, introduzimos o conceito de congruência mostrando suas aplicações e propriedades. Notamos que nesse momento os alunos tiveram mais facilidade com os conceitos apresentados.

Após a explicação dos conteúdos, foram apresentados exemplos e realizados exercícios. A seguir destacamos um dos exercícios que nos chamou a atenção.

O intuito era ensinar aos alunos o "porque"do critério de divisibilidade por 3. Assim, inicialmente, pedimos aos alunos que verificarem se $1353 \equiv 0 \mod 3$, o que foi facilmente visto. Logo após, a seguinte relação foi feita no quadro como mostra a figura 4.3.

$$1.1000 \equiv 1.1 \mod 3$$
$$3.100 \equiv 3.1 \mod 3$$
$$5.10 \equiv 5.1 \mod 3$$
$$3.1 \equiv 3.1 \mod 3$$

Como os alunos sabiam das propriedades de congruência, foi feita a soma dos mesmos obtendo-se o seguinte resultado:

$$1.1000 + 3.100 + 5.10 + 3.1 \equiv 1.1 + 3.1 + 5.1 + 3.1 \mod 3$$
$$1353 \equiv 12 \mod 3$$

ou seja,

$$1353 \equiv 0 \mod 3$$

logo 1353 é divisivel por 3.

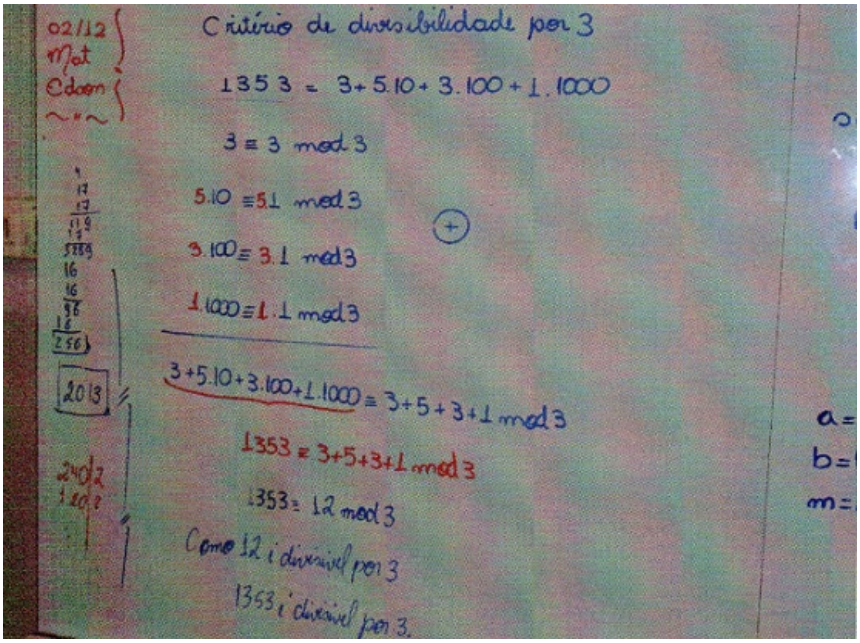


Figura 4.3: Critério de divisibilidade por 3.

Depois desse exemplo prático, os alunos foram levados a investigarem de maneira formal como seria a demostração do critério de divisibilidade por 3, pensando no exemplo feito de maneira genérica. Notamos a grande por parte dos alunos em generalizar o exercício, pois poucos alunos conseguiram formalizar o problema contudo, após socializarmos a demonstração no quadro, todos compreenderam e perceberam que não era tão difícil quanto acharam.

Segue a demonstração apresentada aos alunos:

Seja um número **x** qualquer escrito na base 10. Sabemos que esse número pode ser escrito como $x_n x_{n-1} ... x_0$ ou seja, $x_n.10^n + x_{n-1}.10^{n-1} + ... + x_0$.

Observemos que,

$$10 \equiv 1 \mod 3$$

logo,

$$10^i \equiv 1^i \mod 3$$

ou ainda,

$$x_i.10^i \equiv x_i.1 \mod 3.$$

Daí, podemos afirmar que:

$$x_0 \equiv x_0 \mod 3$$
$$10.x_1 \equiv 1.x_1 \mod 3$$
$$10^2.x_2 \equiv 1.x_2 \mod 3$$
$$\bullet$$
$$\bullet$$
$$\bullet$$
$$10^n.x_n \equiv 1.x_n \mod 3$$

Utilizando as propriedades de congruência temos que,

$$10^n.x_n + ... + 10^2.x_2 + 10.x_1 + x_0 \equiv x_n + ... + x_2 + x_1 + x_0 \mod 3$$

ou seja,

$$x \equiv x_n + ... + x_2 + x_1 + x_0 \mod 3$$

Portanto, para x ser divisível por 3 temos que a soma dos seus algarismos devem ser divisíveis por 3.

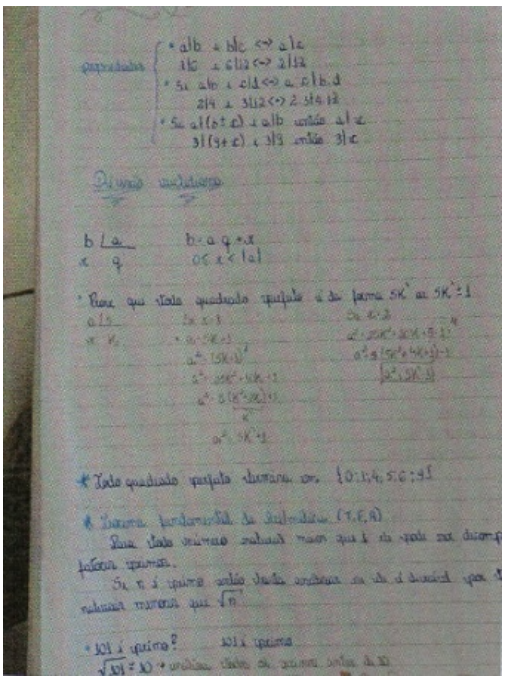


Figura 4.4: Anotações discentes.

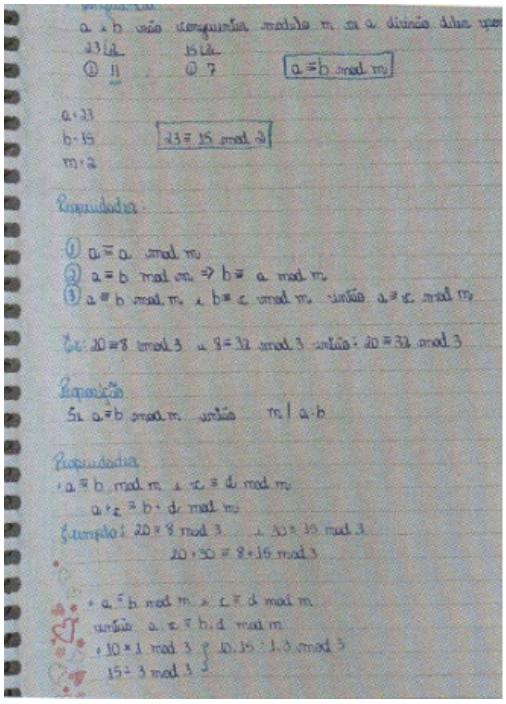


Figura 4.5: Anotações discentes.

4.1.4 Terceira etapa - A importância de divisibilidade e congruência na criptografia

Para a elaboração desta etapa, que teve duração de 1 hora/aula, nos pautamos no capítulo 3 deste texto. Assim, apresentamos aos alunos a importância dos conceitos de divisibilidade e de congruência na criptografia, suas aplicações em Cifras de Translação, Cifras Afim, Cifra de Hill e na Cifra de César.

Perceber a relação entre congruência e criptografia possibilitou que os alunos compreendessem a importância da Matemática para a evolução da sociedade.

4.1.5 Quarta etapa - Codificação e decodificação de mensagens pelos métodos apresentados

A última etapa teve duração de 5 horas/aula e teve como principal objetivo ensinar diferentes métodos criptográficos. Para isso, foram utilizados alguns materiais concretos em busca de estimular o aprendizado por meio da manipulação. Foram necessários copos de diferentes tamanhos e tiras de papel que simularam pergaminhos para melhor explicação da Cítala Espartana assim como, discos concêntricos e tabela de frequência das letras em português para compreensão da Cifra de César e Cifrário por Substituição respectivamente.

Dividimos os participantes em três grupos de aproximadamente 12 alunos e propomos uma competição com algumas atividades.

As atividades propostas tinham como objetivo que cada grupo codificaria mensagens onde os outros grupos as decodificariam. Marcava-se pontos o grupo que conseguisse fazer a decodificação correta da mensagem do outro grupo, no tempo hábil. Um material de apoio foi preparado para algumas atividade como mostrado na figura 4.6. Ao final de cada atividade, realizamos junto aos alunos a cifragem de cada uma das mensagens a serem decodificadas pelos grupos. No que segue, apresentamos algumas atividades desenvolvidas.

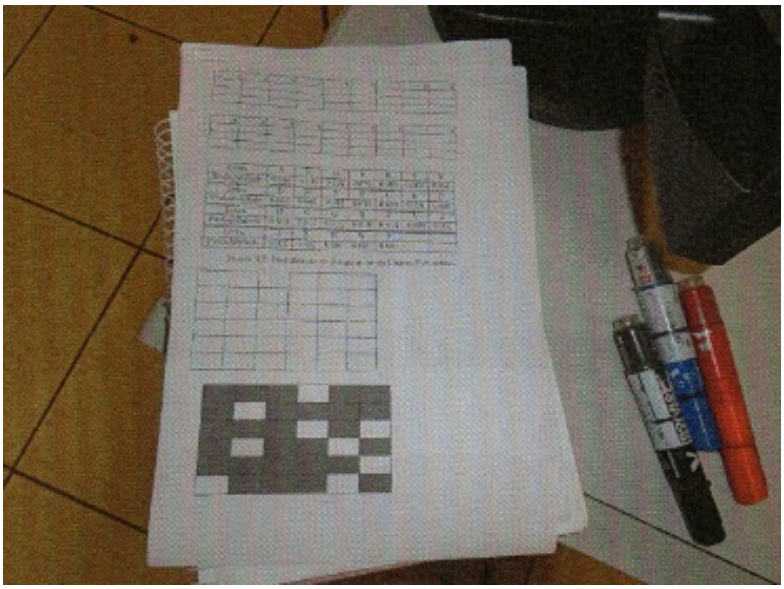


Figura 4.6: material preparatório para as atividades.

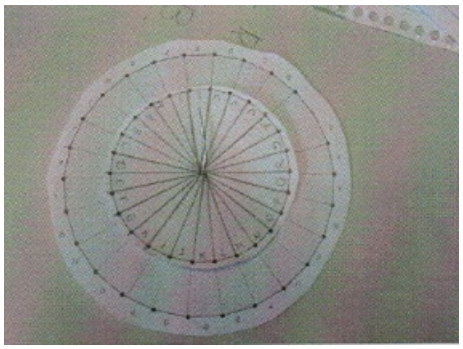
A primeira atividade

Inicialmente, foi feita a construção do disco de cifras por deslocamento. Ela se deu com o auxílio de dois discos concêntricos de raios distintos. Os alunos fizerem a divisão desses em 26 partes iguais correspondentes a cada letra do alfabeto, como podemos verificar na figura 4.8. De acordo com dados históricos, esse método de criptografia foi muito utilizado para criptografar mensagens secretas na guerra civil americana $(1861 - 1865)$.

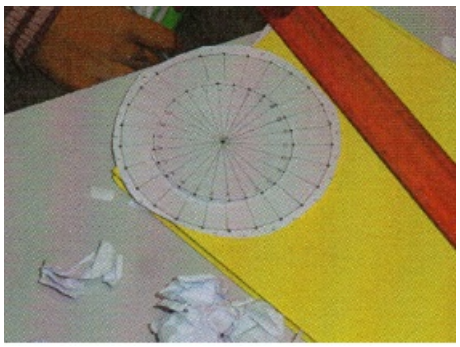
Figura 4.7: Disco de cifras utilizado na guerra civil americana [10]

[10] figura retirada de: http://www.cryptomuseum.com/crypto/usa/ccd/index.htm

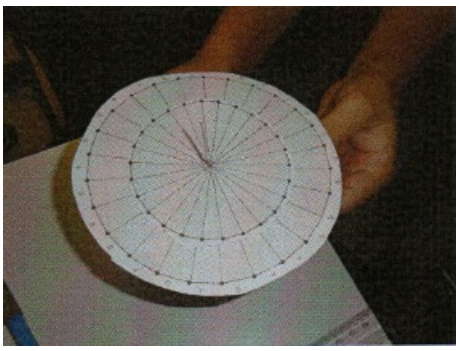
primeira etapa



segunda etapa



terceira etapa



quarta etapa

Figura 4.8: Construção do disco de cifras.

Após a construção do disco de cifras, os alunos efetuaram a codificação de frases escolhidas por eles. Posteriormente, foi feita a decodificação pelos grupos adversários (ver figuras 4.9 e 4.10). Cada grupo deveria informar a chave da codificação E_n e decodificação D_n de cada frase da forma:

$$E_n(x) \equiv (x+n) \mod 26$$
$$D_n(x) \equiv (x-n) \mod 26$$

onde, x representa cada letra do alfabeto da forma $A = 0, B = 1, ..., Z = 25$ e n a translação efetuada no alfabeto (chave da codificação).

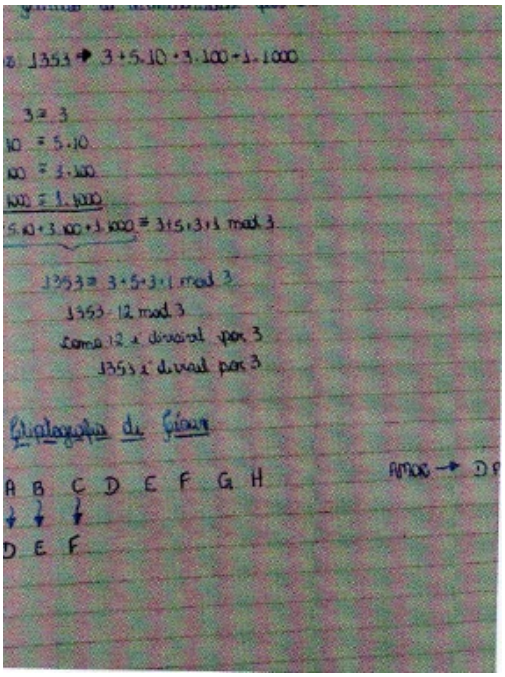


Figura 4.9: Anotações sobre cifra de César.

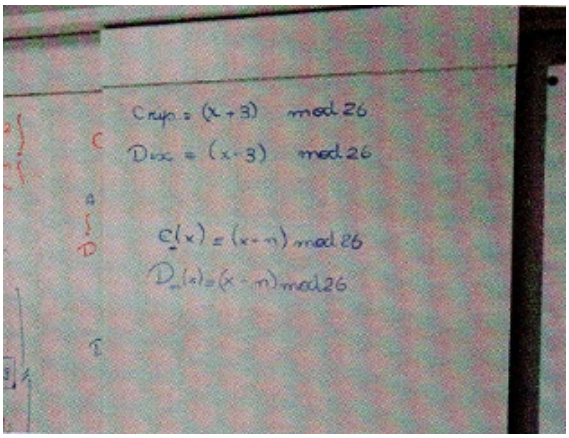


Figura 4.10: Chave da codificação e decodificação.

A segunda atividade

Nessa atividade os alunos fizeram a cifragem de mensagens por transposição colunar como visto na seção 3.4 do capítulo 3. Da mesma forma que na primeira atividade, a escolha das mensagens foram feitas pelos grupos.

As mensagens deveriam ser escritas na forma de matrizes $M_{n\times 9}$, dependendo do tamanho da frase escolhida. A transposição colunar foi pré estabelecida como 423519876 para dar mais dinâmica ao processo.

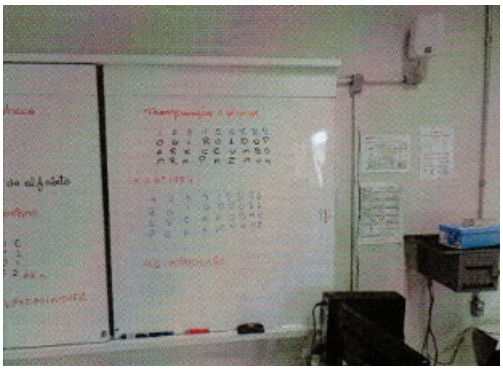
Após os grupos trocarem as mensagens cifradas, os mesmos verificaram que bastava copia-lá novamente em uma matriz $n \times 9$. Após esse processo, devia-se fazer a troca das colunas da mensagem cifrada que estava na ordem 423519876 até que se obtivesse a sequência 123456789 fornecendo assim, a frase decifrada. Foi pedido para os alunos observarem que a ordem pré estabelecida é a chave do processo de codificação e decodificação desse método. Um desses exemplos, podemos observar na figura 4.11, terceira etapa. A frase:

"Não viremos amanhã, estamos de férias".

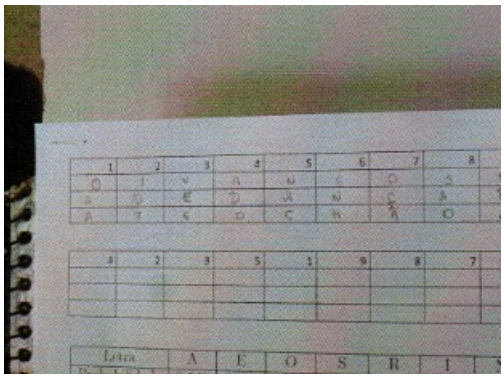
Fica assim codificada quando aplicamos a ordem pré estabelecida:

"VAOINOMER AAMNSSEAH OAMSTEFED SIAXRUWZY".

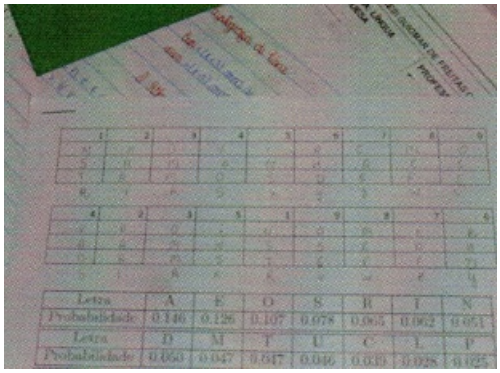
Como podemos verificar na figura 4.11, quarta etapa.



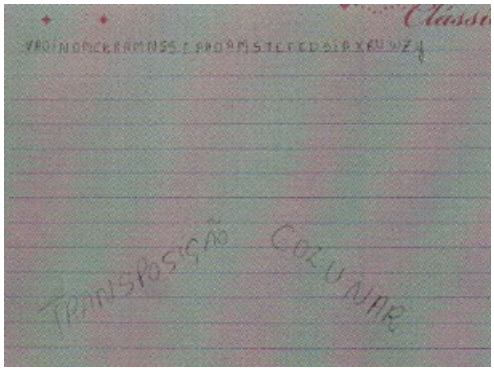
primeira etapa



segunda etapa



terceira etapa



quarta etapa

Figura 4.11: Atividade de cifragem por transposição colunar.

A terceira atividade

Nessa fase foi utilizada a codificação pela Cítala Espartana. Inicialmente foi feita a construção de tiras de papel que representariam os pergaminhos. Logo após, foi escolhida uma frase única para ser codificada pelos grupos. A escolha de uma única frase foi importante para que os alunos observassem que com cilindros diferentes, a codificação também se torna diferente, ou seja, para cada cilindro existe uma matriz associada, como visto na seção 3.4.1 do capítulo 3. Ver figuras 4.12, 4.13 e 4.14.

A frase pré estabelecida foi:

"Índio quer cachimbo, índio quer fazer fumaça".

Associada à uma matriz 6×7 temos:

$$\begin{pmatrix} I & U & H & N & E & R & A \\ N & E & I & D & R & F & A \\ D & R & M & I & F & U & C \\ I & C & B & O & A & M & A \\ O & A & O & Q & Z & A & B \\ Q & C & I & U & E & C & O \end{pmatrix}$$

Que quando codificada nos fornece:

"IUHNERA NEIDRFA DRMIFUC ICBOAMA OAOQZAB QCIUECO".

como podemos observar na figura 4.14.

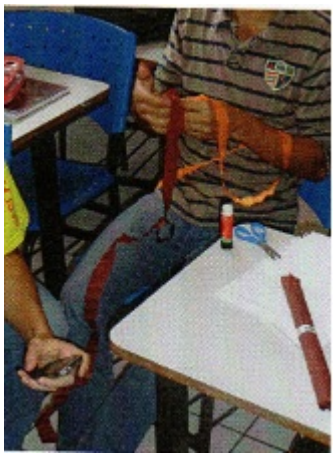


Figura 4.12: Construção do pergaminho

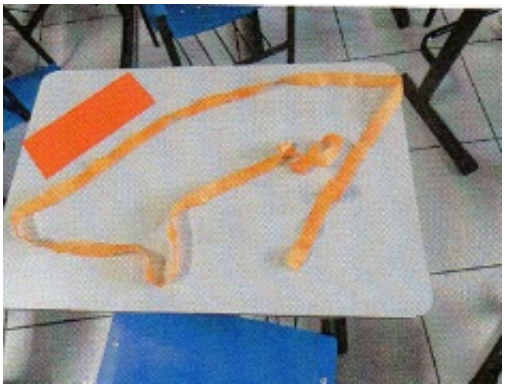


Figura 4.13: Modelo de pergaminho

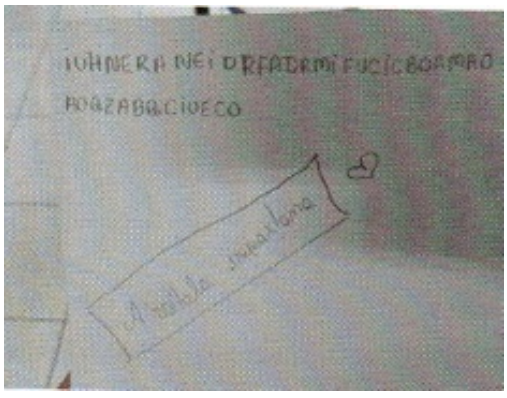


Figura 4.14: Mensagem codificada

A quarta atividade

Na quarta atividade, foi utilizada a criptografia pela Máscara de Matias Sandorf como descrito na seção 3.6 do capítulo 3. Foi pedido para que cada grupo escrevesse uma frase em uma matriz 6×6. Para melhor dinâmica da atividade e melhor compreensão do processo criptográfico, disponibilizamos uma máscara (chave da codificação e decodificação) que faria a codificação da mensagem. Em posse desta máscara, cada grupo deveria fazer a codificação da mensagem por eles escolhida e entregá-la para o grupo adversário, para que este grupo podesse decodificá-la. Após a atividade, cada grupo foi desafiado a desenvolver sua própria máscara de codificação. Ver Figura 4.15.

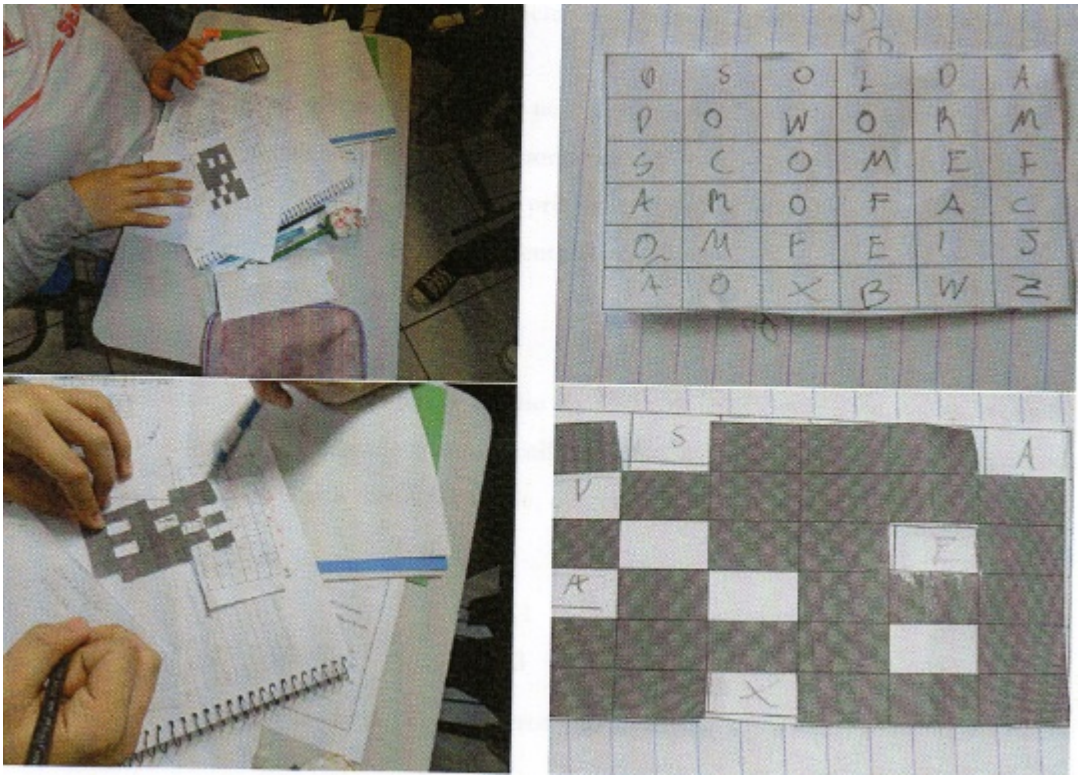


Figura 4.15: Atividade de cifragem por Máscara de Matias Sandorf

A quinta atividade

Na quinta atividade realizada, utilizamos a cifragem por substituição como descrito na seção 3.2 do capítulo 3. Esse método criptográfico possui exatamente 26! maneiras diferentes de serem efetuadas. Com a disponibilização da tabela de frequência de letras do alfabeto (Ver tabela 3.1) para os alunos, eles puderam observar que mesmo com uma grande quantidade de cifragens possíveis, a codificação de uma mensagem por esse método não é seguro.

Nessa atividade, disponibilizamos o mesmo texto cifrado utilizado como exemplo na seção 3.2 do capítulo 3.

TD FGLLQ CORQ EGDG FQ DQZTDQZOEQ RTCTDGL LGDQK
QSTWKOQL RODOFXOK ZKOLZTMQL DXSZOHSOEQK YTSOEORQRT
T ROCOROK QDGK. FTLZQL RODTFLGTL,
ETKZQDTFZT ZGRGL WGLZQDGL RQ DQZTDQZOEQ

Os grupos inicaram suas atividades fazendo a contagem da frequência das letras do texto. Ao terminarem, intuitivamente eles foram trocando as letras de maior frequência do texto pelas letras com maior aparição do nosso alfabeto. Com o auxilio da tabela de frequência de letras, eles passaram a decodificar a mensagem cifrada.

Esse método chamou muito a atenção dos alunos, pois a princípio eles acharam que esta era a maneira mais segura de criptografar uma mensagem, devido a enorme quantidade de possibilidades de cifragem porém, observando o padrão de repetição das letras no texto proposto, e com a fácil decodificação do mesmo, com auxílio da tabela de frequência de letras, esse pensamento foi revogado.

A sexta atividade

A sexta e última atividade foi realizada com o auxílio da Cifra de Hill como descrito na seção 3.2.3 do capítulo 3. Para isto, solicitamos que cada grupo escolhesse uma frase para ser codificada e decodificada por este método. Para maior dinâmica desta atividade, disponibilizamos a seguinte matriz quadrada 2×2 (chave da codificação):

$$M = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix},$$

e a seguinte tabela de substituição de letras por números

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

Diante destas informações, explicamos o funcionamento da Cifra de Hill, conforme visto no capítulo 3. A partir disto, cada grupo cifrou sua mensagem e a entregou para o grupo adversário para que este podesse decifrá-la. Em posse das mensagens cifradas, os grupos foram instigados a descobrir como deveria ser feito a decodificação. Todos responderam que para a decodificação da mensagem seria necessário encontrar a

matriz inversa de M, a qual, eles não sabiam como determiná-la, uma vez que esta não é a matriz inversa "normal", como vista por eles no Ensino Médio. Explicamos que a matriz inversa de M deve ser a matriz M^{-1} em $\mathbb{Z}_{26}$ que satisfaça $M \cdot M^{-1} = I$, onde I é a matriz identidade em $\mathbb{Z}_{26}$. Neste caso, a inversa da matriz chave sugerida é dada por:

$$M^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

Em posse desta matriz, a decodificação foi facilmente estabelecida. Essa atividade gerou um certo desconforto nos alunos por envolver cálculos matriciais.

Aqui segue um exemplo da escolha da frase de um grupo e a codificação feita por eles.

A frase escolhida foi:

"Deus é paz".

Fazendo a substituição letra a letra pelos seus respectivos valores, tem-se que:

Deus é paz = (3, 4, 20, 18, 4, 15, 0, 25).

Utilizando M como chave e efetuando as operações módulo 26 tem-se:

$$\bullet \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 65 \\ 37 \end{pmatrix} = \begin{pmatrix} 13 \\ 11 \end{pmatrix} = \begin{pmatrix} n \\ l \end{pmatrix}$$

$$\bullet \begin{pmatrix} y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 20 \\ 18 \end{pmatrix}$$

$$\begin{pmatrix} y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 364 \\ 186 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \end{pmatrix} = \begin{pmatrix} a \\ e \end{pmatrix}$$

$$\bullet \begin{pmatrix} y_5 \\ y_6 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 4 \\ 15 \end{pmatrix}$$

$$\begin{pmatrix} y_5 \\ y_6 \end{pmatrix} = \begin{pmatrix} 164 \\ 117 \end{pmatrix} = \begin{pmatrix} 8 \\ 13 \end{pmatrix} = \begin{pmatrix} i \\ n \end{pmatrix}$$

$$\bullet \begin{pmatrix} y_7 \\ y_8 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 0 \\ 25 \end{pmatrix}$$

$$\begin{pmatrix} y_7 \\ y_8 \end{pmatrix} = \begin{pmatrix} 200 \\ 175 \end{pmatrix} = \begin{pmatrix} 18 \\ 19 \end{pmatrix} = \begin{pmatrix} s \\ t \end{pmatrix}$$

Dessa forma, a frase,

"Deus é paz".

fica assim codificada,

"NLAEINST".

Para a decodificação da mensagem cifrada, foi utilizada a matriz inversa de M aplicando o mesmo processo esboçado para a codificação.

Capítulo 5

Considerações finais

Esse trabalho me fez observar que é possível implementar o conceito de Teoria dos Números nas aulas do Ensino Médio sem prejudicar o conteúdo programático. A abordagem de conteúdos considerados "abstratos"e de Ensino Superior de uma maneira lúdica faz com que os alunos tenham maior interesse pelo assunto.

Mostrar a importância de como a criatividade acompanha o desenvolvimento da matemática, dando suporte para evoluções tecnológicas atuais, pode fazer com que o aluno aumente sua capacidade de interligar os conteúdos vistos em sala com outras aplicações, conseguindo identificar situações possíveis de utilizar tais conhecimentos.

No ensino de funções, análise combinatória e matrizes e até mesmo probabilidade, a criptografia mostra ser uma aplicação bem interessante, que servirá de ferramenta para proporcionar ao estudante maior motivação para o aprendizado desses conteúdos. Além de ajudar os discentes dando subsídios para aplicações de conteúdos teóricos, esse trabalho também poderá servir como material de apoio para docentes de matemática da Educação Básica. Saber de aplicações vistas por determinados conteúdos dará melhor dinâmica para as aulas, possibilitando a formulação de exemplos práticos sobre os assuntos abordados, trabalhando com novas propostas de aplicações em sala de aula.

Enfim, tentar fazer a ligação de conteúdos vistos no Ensino Médio com conteúdos de graduação, interligando uma abordagem histórica a estes, faz com que os alunos possam desenvolver maior interesse pela matemática. Acredito que pessoas mais interessadas são pessoas mais bem sucedidas, tornando-se assim, profissionais melhores.

Bibliografia

[1] HEFEZ Abrano, *Artitmética*, 1º edição. Coleção Profmat, SBM, Rio de Janeiro, 2013.

[2] SANTOS, José Plínio de Oliveira, *Introdução à Teoria dos Números*, 3ª edição, Rio de Janeiro, IMPA, 2000.

[3] FIARRESGA, Victor Manuel Calhabrês, *Criptografia e Matemática*,Universidade de Lisboa Faculdade de Ciências, 2010. Disponível em:

http://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf. Acesso em 08 de abril de 2014.

[4] MARQUES Cristina Maria, *Introdução à Teoria de Anéis*, Departamento de Matemática-UFMG, 1995. Disponível em: http://www.mat.ufmg.br/m̃arques/Apostila-Aneis.pdf. Acesso em 15 de junho de 2014.

[5] SIDKI, Said, *Introdução à Teoria dos Números*. Disponível em: http://www.impa.br/opencms/pt/biblioteca/cbm/10CBM/10_CBM_75_09.pdf. Acesso em 03 de janeiro de 2014.

[6] KOBLITZ, Neal, *A Course in Number Theory and Cryptography*, 2ª ed. Editora Springer-Verlag, 1987.

[7] ALMEIDA, Paulo J., *Criptografia e segurança*. Departamento de Matemática de Aveiro. Portugal, 2012.

[8] FALEIROS, Antonio Cândido, *Criptografia*. Centro de Matemática, Computação e Cognição Universidade Federal do ABC, Santo André, São Paulo, 2010.

[9] MALAGUTTI, Pedro Luiz, *Atividades de Contagem a partir da Criptografia*. IMPA, Rio de Janeiro, 2012.

[10] BUCHMANN, Johannes, *Introdução à Criptografia*, Editora Berkeley, São Paulo, 1ª ed., 2002.