UNIVERSIDADE FEDERAL DA GRANDE DOURADOS -UFGD

FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGIAS – FACET

MARCIA SHIZUE MATSUMOTO

DESPERTANDO O INTERESSE DO ALUNO PELA MATEMÁTICA COM A CRIPTOGRAFIA

DISSERTAÇÃO DE MESTRADO EM MATEMÁTICA

DOURADOS/MS

MARÇO/2014

MARCIA SHIZUE MATSUMOTO

DESPERTANDO O INTERESSE DO ALUNO PELA MATEMÁTICA COM A CRIPTOGRAFIA

ORIENTADOR: LINO SANABRIA

Dissertação de mestrado submetida ao programa de pós-graduação Mestrado Profissional em Matemática, como um dos requisitos necessários para a obtenção do título de mestre em Matemática.

DOURADOS/MS
MARÇO/2014

MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO UNIVERSIDADE FEDERAL DA GRANDE DOURADOS
FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Termo de Aprovação

Após a apresentação, arguição e apreciação pela banca examinadora, foi emitido o parecer APROVADO, para a dissertação intitulada:" **Despertando o interesse do aluno pela matemática com a criptografia",** de autoria de Marcia Shizue Matsumoto, apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal da Grande Dourados.

Prof. Dr. Lino Sanabria (Orientador-UFGD)
Presidente da Banca Examinadora

Prof. Dr. Sérgio Rodrigues
Membro Examinador (UFGD)

Prof. Dr. Vando Narciso
Membro Examinador (UEMS)

Dourados/MS, 31 de março de 2014

Agradecimentos

Eu agradeço a Deus por tudo o que tens feito, pelas oportunidades que me tens dado e pelo amor que tens a mim.

A minha família por ser minha base, pelo amor e apoio de sempre. Ao meu pai Mario pelo incentivo aos estudos, pelos bons ensinamentos, pelas correções, pela educação e pelo caráter. A minha mãe Teresa minha maior defensora, pelo cuidado, dedicação e pela força. A minha irmã Mirian pela companhia, parceria e cumplicidade.

Ao professor Dr. Lino pela orientação, pela confiança, disponibilidade e por toda ajuda na elaboração deste trabalho, sempre com explicações esclarecedoras. Muito Obrigada mesmo pela imensa paciência comigo.

Aos meus professores do mestrado, pelo exemplo e pela dedicação.

Aos professores Sergio Rodriguês e Vando Narciso pela disponibilidade em participar da banca.

A todos que direta ou indiretamente contribuíram para a conclusão deste trabalho.

RESUMO

Geralmente a matemática é vista pelos alunos como um conteúdo antigo, que nunca muda e que não tem ligação com o cotidiano e aplicabilidade em praticamente nada. A criptografia ou escrita escondida surgiu há muitos anos e desde então vem se aprimorando para melhor proteger informações. Hoje em dia é utilizada principalmente na internet para proteger senhas, número de cartão entre muitos outras formas.

Conhecer como ela surgiu com a Cifra de César e como ela tem ligação com a matemática pode levar os alunos a se interessarem pelo conteúdo e refletirem o quanto ele é realmente importante.

Esse trabalho apresenta várias atividades relacionadas a criptografia, são atividades diferentes daquelas apresentadas rotineiramente, portanto pretende-se com elas despertar o interesse do aluno para a matemática.

SUMÁRIO

Figuras

Capítulo 01

1.1 Introdução

Para aprendermos precisamos estar motivados, ou seja, a motivação norteia nosso aprendizado. Em geral a matemática não está no foco da maioria dos estudantes. Falta atenção para os conteúdos, também não fazem nenhuma ligação com o cotidiano. Em geral reclamam muito que não há necessidade nenhuma para estudar matemática, pois em que momento da vida irá utilizar os conceitos matemáticos. Esse mesmo aluno hoje está totalmente concentrado em tudo que está relacionado à alta tecnologia. Ficam conectados praticamente o tempo todo na internet. A maioria das informações que estão presentes nesse meio de comunicação é de livre acesso, ou seja, qualquer pessoa pode ler. Mas tem uma parte que deve ser protegida, como e-mails pessoais, senhas, número de cartão de crédito para a realização de uma compra, entre outros.

A criptografia é o estudo de codificar e decodificar informações para proteger informações pessoais ou interesses de um determinado grupo.

Fazer com que o aluno reflita como a matemática é ferramenta para que muito da tecnologia funcione pode ser um caminho para que ele se interesse mais pelos conteúdos matemáticos.

Hoje a criptografia é usada no mundo inteiro e tem basicamente a mesmo objetivo, que é manter a segurança de informações sigilosas.

Este trabalho apresenta atividades relacionadas ao tema criptografia. São atividades montadas baseadas na origem da Criptografia com a Cifra de César. Consiste em conhecer a história da mesma e entender como ela funcionava. Para a realização das atividades de criptografar mensagens serão confeccionados materiais para facilitar o trabalho e levar o aluno ao melhor entendimento de como funciona o método. Essa seqüência de atividades pretende despertar o interesse do aluno, pois tem ligação com temas atuais e aplicabilidade no cotidiano.

O capítulo dois é voltado para o planejamento do professor, ou seja, usaremos conceitos matemáticos que não fazem parte do currículo dos alunos no ensino fundamental.

Uma parte da seqüência didática foi aplicada nas turmas de 6º e 7º da Escola Municipal Elza Farias Kintschev Real no bairro Cohab II, na região periférica na cidade de Dourados, estado de Mato Grosso do Sul. A escola atende alunos do a partir do 4º ano até o 8º ano do Ensino Fundamental.

1.2 Justificativa

Devido uma resistência por parte dos alunos, na disciplina de matemática, estes adquirem uma rejeição, na qual afirmam que a matemática é difícil, desse modo

faz-se necessário o estudo de novas metodologias que modifiquem ou pelo menos amenizem esta idéia, despertando no aluno um novo olhar para o ensino de matemática. Todavia, há a necessidade de buscar alternativas que sane as dificuldades encontradas no processo ensino-aprendizagem, pois ensinar matemática é desenvolver o raciocínio lógico, estimular o pensamento independente, a criatividade e a capacidade de resolver problemas.

Entretanto, para tal objetivo, as tendências na educação matemática são ferramentas que antecedem a prática, estimulando o ensino da matemática como algo concreto, presente no cotidiano dos alunos. Essa sequencia didática busca aumentar o interesse dos alunos através da ligação da matemática com o cotidiano, pois mostra a eles que a matemática não é somente para dificultar a vida deles, como a maioria acredita, mas que possui imensa aplicabilidade na vida cotidiana.

Neste sentido, propõe atividades que busquem justificar o uso de diversos conteúdos da matemática no cotidiano, induzir nos jovens o gosto e o prazer de estudar Matemática; estimular o ensino e aprendizagem da Matemática no Ensino Fundamental.

De acordo com os Parâmetros Curriculares Nacionais a Rede Municipal de Ensino fez a Proposta Curricular de Dourados-MS. Então todas as escolas Municipais seguem a mesma. Os conteúdos estão divididos em quatro blocos: Números e Operações; Espaço e forma; Grandezas e Medidas e Tratamento da informação. Cada bloco está dividido em quatro bimestres.

Entre os objetivos que estão nos Parâmetros Curriculares Nacionais que podemos contemplar nas atividades relacionadas aqui estão:

Ampliar e construir novos significados para os números naturais a partir de sua utilização no contexto social, pois leva o aluno a perceber a sua importância.

Também reconhecer como as representações algébricas permitem expressar generalizações sobre propriedades das operações aritméticas, no caso $ax + b$.

As atividades serão aplicadas nas turmas de quarto, sexto e sétimo anos.

As atividades para o 6º ano são focadas na adição e multiplicação.

- Adição
- Multiplicação
- Expressões numéricas com adição e multiplicação
- Ângulos
- Circunferências (Construção dos discos)
- Máximo divisor comum (MDC)

No 7º ano podemos explorar a idéia de expressões.

- Equações
- Valor numérico de uma expressão algébrica

Capítulo 02- Criptografia

2.1 Conceito

Desde quando o homem se organizou para viver em grupo ele sentiu a necessidade de guardar informações. Tão forte quanto a necessidade nata da espécie humana de guardar segredos sobre determinados assuntos é a vontade dos mesmos humanos em desvendar esses segredos. Sejam segredos individuais ou coletivos. Com o avanço cada vez maior dos poderes das Redes de Computadores, o mundo tende a ficar menor, perder fronteiras, encurtar distâncias. Hoje, com um simples apertar de teclas, pode-se intercambiar informações através dos cinco continentes em questão de minutos até segundos.

A maioria das informações está aberta a todos, ou seja, não há problemas algum que todos saibam, como por exemplo: notícias de jornais e revistas. Mas também há aquelas informações que não podem estar abertas para todos, são informações sigilosas que pertencem a uma determinada pessoa ou a um limitado grupo de pessoas. Como exemplos : senhas em geral, número de cartão de credito entre muitos outros. Proteger essas informações que é o estudo da Criptografia.

Na palavra criptografia, Cripto vem do grego “Kryptos” e significa oculto, envolto, escondido. Também do grego “graphos” significa escrever. No dicionário Aurélio temos o seguinte significado: Arte de escrever secretamente por meio de abreviaturas ou de sinais convencionados entre duas ou mais pessoas ou partes. Codificação de um artigo ou outra informação armazenada num computador, para que só possa ser lido por quem detenha a senha de sua decodificação.

A Criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-lo. É a ciência que oculta o significado de uma mensagem e têm como ferramenta os recursos matemáticos para encriptar mensagens. O ato de encriptar consiste em transformar um texto normal em texto secreto. É também uma ciência matemática que se dedica ao estudo de métodos de comunicação secreta. É composta pelas disciplinas de criptografia e criptoanálise.

O fundamental propósito da criptografia é permitir a transmissão de mensagens por canais não seguros empregando técnicas matemáticas para tornar o conteúdo da mensagem restrita ao destinatário legitimo. É uma ciência tão antiga quanto a própria escrita, porem somente depois da Segunda Guerra Mundial, com a invenção do computador e o desenvolvimento da teoria da informação a criptografia realmente evoluiu.

2.2 História

A escrita por meios de códigos começou a ser conhecida pelo relato feito por Heródoto, um historiador romano, por volta do quinto século antes de Cristo, que relatou os conflitos ocorridos entre a Grécia e Pérsia. Nesta batalha se lutava pela liberdade, onde a escrita foi fundamental na guerra. A estratégia utilizada pelos Persas foi organizarem secretamente um exercito militar para combater a Grécia, seu plano era o ataque surpresa. No entanto não contavam que a Grécia usasse uma arma muito forte que era a arte da escrita secreta. O grego Demerato que morava na Pérsia, escreveu em um par de tabuletas raspando a cera e escrevendo a mensagem. Depois a escrita a cobria novamente para assim ser passada pelos guardas sem ser descoberta. Com isso em 23 de setembro de 480 a.C. Xerxes líder dos Persas atacou a Grécia que o esperava bem preparada. Assim Xerxes perdeu a batalha pelo fato de não ter realizado o combate de forma surpresa. Esse tipo de criptografia, ocultação de mensagem, é conhecido como esteganografia originada da palavra grega steganos (coberto) e graphein (escrever).

A criptografia mais conhecida surgiu nas Guerras da Gália de Júlio César, e por este motivo ficou conhecida como Cifra de césar. Ele substituía cada letra na mensagem por outra que estivesse três casas à frente no alfabeto.

Criptografia por substituição era muito usada, o que tornava conhecida o seu método de cifrar e decifrar sendo de fácil acesso a descoberta da mensagem criptografada. Com isso surgiu uma nova forma criptografia feita por substituição criada por Blaise de Vigenère em 1563. Baseada não apenas em um, mas sim em 26 alfabetos cifrados. Essa por sua vez é denominado de cifra polialfabética, e foi utilizado por muito tempo, sendo quebrada somente em 1854. Durante muitos outros anos nenhum outro método de criptografia foi desenvolvida com tanta segurança.

Somente em 1918, o alemão Arthur Sherbius desenvolveu uma nova forma de criptografar. Ele construiu uma maquina cifrante, chamada Enigma, que era composta de três elementos: um teclado para introduzir a mensagem; um misturador que permutava o alfabeto: um mostrador para visualizar mensagem cifrada.

Figura 01- Máquina Enigma

Aqui se inicia a troca das cifras de papel e lápis por uma mais moderna que utilizava a tecnologia do inicio do século XX. Em 1926 o exército alemão a utilizou fazendo algumas modificações obtendo a rede de comunicação mais segura da época. Em 1940 Alan Turing e sua equipe da inteligência britânica construíram o primeiro computador operacional e seu propósito especificamente era decifrar mensagens alemãs cifradas pela Máquina Enigma. Esta primeira maquina foi substituída em 1943, recebendo o nome de Colossus, com a tecnologia de válvulas era capaz de realizar diversos cálculos capaz de quebrar códigos da máquina Enigma.

Após a Segunda Guerra Mundial com o desenvolvimento de computadores e outras tecnologias a criptografia foi tornando-se mais complexa. Em 1977 a equipe Rivest, Shamir e Adleman desenvolveram um estudo de criptografar usando uma função de mão única. Composta de duas chaves diferentes, uma delas publica que visa: a autenticação de destino, que garante que somente o destinatário consiga ler a mensagem; a autenticação da origem, que evita a falsificação da identidade do emissor; a detenção de integridade de informação que evita outra pessoa leia e altere a informação. A outra é a chave privada que é usada para decifrar a mensagem, assim esse algoritmo é chamado algoritmo assimétrico. A importância deste tipo de sistema é que viabiliza a troca de informações, de forma segura, via internet. Essa criptografia ficou conhecida como RSA, onde basea - se em função modular e conhecimento em teoria dos números. Nos tempos de hoje utilizasse sistemas de criptografia de chave publica, onde as chaves são números com ordem de grandeza elevado. Este é o ponto chave da segurança destes sistemas, pois, “todos os computadores do planeta levariam mais tempo do que a idade total do universo para quebrar a cifra”.

Com essa breve historia da criptografia percebe-se que tanto a matemática quanto a criptografia estão interligadas, sendo que esse processo é continuo, onde a criptografia moderna é definida a partir do algoritmo aplicado, que este por sua vez é definido pelo desenvolvimento ocorrido nas disciplinas aplicadas.

Nesse trabalho estudaremos a Cifra de César mais detalhadamente e as atividades serão baseadas na encriptação pelo deslocamento das posições das letras e também pelo deslocamento utilizando funções do tipo $ax + b$.

2.3 Cifra de César

A Cifra de César é feita por substituição. Ela substitui uma letra por outra três posições à frente no alfabeto.

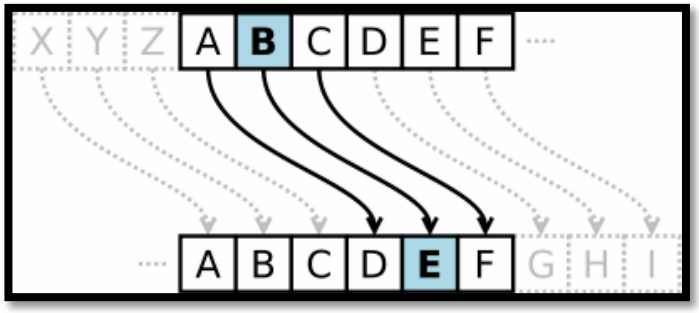


Figura 2

Com o advento do computador todos os processos de encriptação têm algum processamento numérico, por isso vamos fazer a substituição das letras do alfabeto por números, da seguinte:

$$A \rightarrow 0$$

$$B \rightarrow 1$$

$$C \rightarrow 2$$

$$D \rightarrow 3$$

$$E \rightarrow 4$$

$$F \rightarrow 5$$

$$G \rightarrow 6$$

$$H \rightarrow 7$$

Sucessivamente até

$$Z \rightarrow 25$$

Assim a Cifra de César pode ser vista como uma adição no conjunto de números que representam as letras do alfabeto, a saber:

$$x \rightarrow x + 3$$

Como dar sentido a $25 + 3 = 28$? Ora, essa resposta já está definida pela substituição $25 \leftrightarrow Z \leftrightarrow c \leftrightarrow 2$.

Do ponto de vista matemático, estamos trabalhando com soma modulo 26, isto é, a operação está definida no conjunto $Z_{26} = \{0, 1, \ 2, \ldots 25\}$ da seguinte forma.

$$x + y = (x + y) mod\ 26$$

Isto coloca em evidência que a cifra de César é uma função de Z_{26}em Z_{26}, definida por:

$$f: Z_{26} \rightarrow Z_{26}$$

$$x \rightarrow x + 3$$

É claro que nas séries iniciais não será este o ponto de vista adotado, mas todas as atividades podem ser vistas como uma preparação para estes temas. E nas séries finais do ensino médio já podem ser abordadas, sem o rigor de um curso de álgebra.

A generalização da Cifra de César pode então ser definida do seguinte modo:

$$f: Z_{26} \to Z_{26}$$
$$x \to x + k$$

Não é difícil verificar que a inversa de f é dada por $f^{-1}(x) = x + k'$, onde $k + k' = 26$. Observe que se $k = 0$ a função f é uma identidade, a qual não nos interessa encriptar. As tentativas para decriptar serão bem sucedidas com no máximo 25 tentativas.

Na próxima seção vamos introduzir uma variação na Cifra de César que tornara mais interessante nosso problema de encriptar e decriptar.

2.4 Cifra de César estendida.

Em vez de simplesmente fazer um deslocamento, faremos uma multiplicação seguida de um deslocamento, ou seja, vamos definir a função de Z_{26} em Z_{26} pondo$f(x) = ax + b$, com $a \neq 0$.

Para que esta função seja uma função de encriptação ela precisa ser inversível, pois quando fazemos a decriptação se ela não for inversível, dois elementos diferentes podem representar a mesma letra. A condição para que uma função seja inversivel é que ela seja bijetora.

Como na função $f: A \to A$, A é finito,temos que $f \text{ é } injetiva \leftrightarrow f \text{ é } sobrejetiva$. Portanto, para que esta função seja uma função de encriptação é necessário (e suficiente) que seja injetiva.

Basta fazer algumas experimentações atribuindo valores para *a*, para perceber que em alguns casos a função não será injetiva. Mais, precisamente, temos:

Proposição: A função $f: Z_{26} \to Z_{26}$, dada por $f(x) = ax + b$ é injetiva, se e somente se, $mdc(a, 26) = 1$

Faremos a demonstração da contra-positiva, isto é vamos mostrar que:

$$mdc(a, 26) \neq 1 \to f \text{ não é } injetiva$$

Suponha que $mdc(a, 26) = d$ e que $d > 1$, então temos que $a = a' \times d$. Logo $26 = x_0 \times d$ com $1 < x_0 < 26$.

$$f(x_0) = a \times x_0 = a' \times d \times x_0 = a' \times 26 = 0(mod\ 26)$$

Portanto temos que $f(0) = 0 = f(x_0)$. Portanto a função não é injetiva.

$$mdc(a, 26) = 1 \to f \text{ é } injetiva$$

Se $mdc(a, 26) = 1$, então existem a' e b em N tais que $1 = a'.a + b.26$, isto é, $a'.a = 1\ mod\ 26$. Somando um múltiplo positivo de 26 a x. Sejam $x\ e\ y$ tais que $f(x) = f(y)$, isto é, $ax = ay$. Temos $a(x - y) = 0$. Multiplicando por a'.

$a'.a(x - y) = 0$. Como $a'.a = 1\ mod\ 26$, temos que $(x - y) = 0$, isto é $x = y$. Portanto f é injetiva.

Exemplo: Seja $f(x) = 2x$.

Sabemos que $mcd(2,26) = 2$

Temos que $26 = 13 \times 2$. $f(13) = 2 \times 13 = 26 = 0(mod\ 26)$. Portanto temos que $f(0) = f(13) = 0$.

- $f(x) = ax + b$ é injetiva se *a* é invertível em Z_{26}.

$f(x) = f(y) \leftrightarrow a(x - y) = 0 \leftrightarrow a^{-1}.a(x - y) = 0 \rightarrow x = y$

$x \neq y \qquad f(x) = f(y) \rightarrow a(x - y) = 0$ implica a não é invertível.

Problema: Como determinar a inversa de $f(x) = ax + b$?

Seja f^{-1} a inversa de f, então $f\left(f^{-1}(x)\right) = a.f^{-1}(x) + b = x$

$a.f^{-1}(x) = x.b'$, onde $b + b' = 26$. Basta agora determinar o inverso de a. Daí

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

$$f^{-1}(x) = a^{-1}x + a^{-1} \times b'$$

Para determinar o inverso podemos usar o algoritmo de Euclides. Vamos exemplificar calculando o inverso da função: $y = 17x + 5$

$$y + 21 = 17x$$

$$17x = y + 21$$

Calculando o mdc(17,26)

$$26 = 1 \times 17 + 9$$

$$17 = 1 \times 9 + 8$$

$$9 = 1 \times 8 + 1$$

Logo mdc(17,26)=1

$$1 = 9 - 8$$

$$1 = 9 - (17 - 9)$$

$$1 = 9 + 9 - 17$$

$$1 = 2 \times 9 - 17 = 2(26 - 17) - 17$$

$$1 = 2 \times 26 - 3 \times 17$$

$$1 = 2 \times 26 + (-3) \times 17$$

Temos que $-3 + 26 = 23$

$$23 \times 17x = 23y + 21 \times 23$$

$$x = 23y + 15$$

Portanto a inversa de $y = 17x + 5$ é $y^{-1} = 23x + 15$

2.5- Criptoanálise

Enquanto a Criptografia trata de tornar as mensagens secretas, por outro lado existe também a "***Criptoanálise***", que é a arte de "*quebrar*" os criptogramas, recuperando as mensagens, mesmo sem se conhecer a chave apropriada para a decifragem. Por isto, os algoritmos criptográficos devem satisfazer a uma série de critérios de forma a garantir, no maior grau possível, que seja impraticável *quebrar* o sistema.

A criptoanálise desenvolveu durante a era medieval técnicas de análise de freqüência, na qual as freqüências das letras na mensagem são comparadas às freqüências médias em textos do idioma da mensagem, permitindo quebrar com facilidade cifras de substituição. Dado o baixo requerimento computacional da análise de freqüência, as cifras clássicas são consideradas atualmente como incapazes de fornecer qualquer segurança real, sendo utilizados apenas como formas ocasionais de entretenimento.

A partir do início do século XX começou-se a usar aparelhos mecânicos para aplicar e remover cifras, combinando mensagens em texto puro, chaves secretas e operações matemáticas. A Segunda Guerra Mundial foi prolífica em métodos criptográficos e aparelhos para quebra de cifras; a máquina Enigma tornou-se célebre por ser usada pelo exército alemão durante a guerra e por ter tido sua cifra quebrada pelos aliados, que descobriram segredos militares alemães.

Entre as décadas de 1950 e 1970 a criptografia foi tratada como segredo de estado e muito pouco foi divulgado; suas evoluções voltaram a ser públicas na década de 1970, fundamentadas sobre as teorias de matemática, informação e comunicação e calcadas nos computadores digitais.

Códigos de César padecem de um grande mal, são muito fáceis de decifrar. Na verdade qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto se deve ao fato de que a freqüência média com que cada letra é usada em uma língua é mais ou menos constante. Por exemplo:

- As vogais são mais freqüentes que as consoantes;
- A vogal mais freqüente é o A;
- Se um monossílabo tem uma única letra, então esta letra é uma vogal;
- Consoantes como S e M são mais freqüentes que as outras;

Assim, apenas contando a freqüência de cada símbolo no texto, podemos descobrir a que letra corresponde os símbolos mais freqüentes. Isto geralmente é suficiente para decifrar toda a mensagem. Observe, entretanto, que este método só

funciona se a mensagem for longa. É fácil escrever uma mensagem curta cuja contagem da freqüência seja totalmente diferente da contagem média do português.

Decifrar uma mensagem por contagem de freqüência é mais simples se temos um computador. Supondo que a língua é conhecida, a maior parte do processo pode ser automatizado. Isto torna essencialmente inviáveis todos os códigos que envolvem substituições de letras. Na verdade, alguns dos primeiros computadores foram montados exatamente para auxiliar na decifração dos códigos secretos usados pelos alemães durante a 2ª Guerra Mundial.

Hoje em dia, a comunicação entre computadores pela Internet vem criando novos desafios para a criptografia. Como é relativamente fácil interceptar mensagens enviadas por linha telefônica, torna-se necessário codificá-las, sempre que contenham informações sensíveis. Isto inclui transações bancárias ou comerciais, ou até mesmo compra feita com cartão de credito.

Assim tornou-se necessário inventar novos códigos, que fossem difíceis de decifrar, mesmo com a ajuda de um computador. No código usado por César, se você sabe codificar, então também sabe decodificar. Mas essa codificação não é mais utilizada hoje em dia. Mas como esse tema não é o foco do trabalho não será relevante as atividades deste trabalho.

Capítulo 03- Proposta Metodológica

3.1 Confecção dos discos

Vamos considerar a afirmação: “um dia tem 24 horas”, do ponto de vista matemático. Ora, um dia de 24 horas é uma subdivisão arbitrária e imaginaria de um conjunto contínuo de tempo. Podemos descrever isto matematicamente do seguinte modo. Fixamos um momento inicial a partir do qual o tempo é contado. A seguir estabelecemos uma relação de equivalência: dois momentos que diferem por 24 horas correspondem a horas análogas em dias diferentes. Queremos fazer uma coisa semelhante não com a sucessão das horas, mas com o alfabeto que é um conjunto finito de 26 letras e relacioná-lo com o conjunto dos números naturais.

A correspondência que relaciona o alfabeto ao conjuntos dos números naturais inicia-se a partir do 0. Associamos cada letra a um número, A se relaciona com o 0, o B com o 1 e assim por diante até o Z que se relaciona ao número 25. Mas podemos fazer transformações que levam a números maiores que o 25. Com isso temos que 26 é levado em 0, 27 é equivalente a 1.

A forma mais prática de representação de um conjunto finito que se corresponde a outro conjunto infinito é um círculo, pois o mesmo apresenta um ciclo de 360º, mas podemos representar ângulos maiores que 360º.

O disco facilita o trabalho de criptografar, pois como ele apresenta um ciclo, se o resultado da transformação, ou seja, da encriptação do valor de cada letra for maior que 26 mesmo assim temos seu respectivo correspondente. O que não acontece com uma tabela linear por exemplo.

Para a confecção do disco seguimos os seguintes passos:

Para essa atividade será necessário:

- Papel cartão (duas cores)
- Colchetes (broches)
- Canetinhas
- Compasso
- Régua
- Compasso

1º passo: Construir em papel cartão duas circunferências de raios diferentes. (uma maior que a outra).

2º passo: Dividir as duas circunferências em 26 partes iguais, cada parte corresponde a uma letra do alfabeto.

Nesse passo apresenta-se uma dificuldade: Quando dividimos 360 graus em 26 partes iguais, o resultado é 26 graus e 50 minutos. Essa medida não é construtível no compasso. Portanto precisamos utilizar um software para desenhar a circunferência dividida em 26 partes iguais. (figura 3). Colamos a figura na circunferência de modo que elas fiquem concêntricas. Basta ligar com uma régua o centro a extremidade da circunferência.

3º passo: Prendemos com um colchete as duas circunferências de modo que elas fiquem concêntricas elas girem independentes uma da outra. A menor será o conjunto de partida e a maior o conjunto imagem.

Iremos confeccionar dois discos:

1º- Leva letras em letras-

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

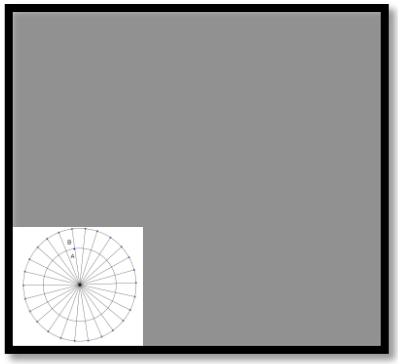


Figura 3

2º Leva letra em números

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

Nesse parte do planejamento podemos confeccionar todos os discos que serão usados nas próximas atividades.

Figura 4

Para decriptar uma mensagem se faz necessário o cálculo das funções inversas e como as atividades serão realizadas nos anos do ensino fundamental se faz necessário a confecção de todos os discos que iremos utilizar, pois os alunos nessa idade escolar não sabem esse conteúdo. No caso das atividades propostas nessa seqüência didática são os discos:

- $y = 3x + b$
- $y = 5x + b$
- $y = 7x + b$
- $y = 9x + b$
- $y = 11x + b$
- $y = 15x + b$
- $y = 17x + b$
- $y = 19x + b$
- $y = 21x + b$
- $y = 23x + b$
- $y = 25x + b$

3.2- Plano de aula

3.2.1- Apresentação da história da Criptografia para os alunos.

Nessa atividade os alunos conhecerão através do seguinte texto a história da criptografia. Também iremos fazer alguns exercícios para a melhor fixação do texto.

Criptografia

A palavra criptografia surgiu da fusão das palavras gregas "kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Consiste em várias técnicas para esconder informações de acesso não autorizado. Seu principal objetivo é codificar e decodificar dados e informações sigilosas.

Hoje em dia ela se torna necessária para proteger as informações que enviamos principalmente pela internet. Também utilizada em senhas de bancos e proteção de informações.

Antigamente, a cifragem era utilizada na troca de mensagens, sobretudo em assuntos ligados à guerra. Por milênios, generais, reis e rainhas buscavam formas mais eficientes de comunicação. Isso era necessário para comandar seus exércitos e para governar seus países. A extrema importância de não revelar segredos e estratégias as forças inimigas levou ao estudo e motivou o desenvolvimento de códigos e cifras, técnicas para comunicar de forma que apenas o destinatário seria capaz de ler a mensagem.

Estudaremos a Cifra de César, que é uma das mais simples e conhecidas técnicas de criptografia. Consiste na técnica de substituição de cada letra do alfabeto abaixo dela um número exatamente três vezes.

Exemplo:

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

Exercícios

01- Usando a Cifra de César, criptografar as seguintes mensagens:

a) A matemática é o alfabeto com o qual DEUS escreveu o universo. (*Pitágoras).*

b) O único lugar onde o sucesso vem antes do trabalho é no dicionário. (*Albert Einstein*)

3.2.2 Atividade 2

Encriptar e Decriptar palavras usando a Cifra de César

Nessa atividade iremos encriptar e decriptar palavras utilizando a Cifra de César. Iremos dividir a sala em vários grupos. Cada aluno irá receber uma palavra e irá escolher o deslocamento, ou seja, irá escolher o valor do b.

Criptografar a seguinte palavra utilizando a Cifra de César, escolha o deslocamento.

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

ESCOLA_____

Criptografar a seguinte palavra utilizando a Cifra de César, escolha o deslocamento.

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

MATEMÁTICA_____

Criptografar a seguinte palavra utilizando a Cifra de César, escolha o deslocamento.

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

ESTUDAR_____

Depois eles irão trocar as palavras cifradas para cada grupo descobrir as palavras dos outros grupos.

Quando apenas deslocamos uma quantidade k nas letras é possível descobrir fazendo todas as possibilidades seguindo a ordem do alfabeto.

Podemos usar esse processo quando temos apenas uma palavras e quando o valor do a é igual a zero.

Exemplo:

Decriptar a palavra KYIURG.

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

3.2.3 Verificar quais números a que funcionam na Cifra de César estendida

Verificando quais números podem ser usados para criptografar na forma $(\boldsymbol{ax+b})$.

Com o disco de criptografar que leva cada letra do alfabeto em números podemos perceber que podemos não somente deslocar casas a frente, podemos multiplicar um número depois somar. Se o número obtido for maior que 25, dividimos esse número por *26* e consideramos o seu resto. Com a tabela logo em seguida, o cálculo se torna mais rápido. Podemos perceber que através dessa tabela podemos concluir que *0= 26= 78=104* e assim por diante, pois como as letras vão de zero a vinte e cinco, no vinte e seis começa-se um novo ciclo.

Podemos exemplificar esse conceito com o seguinte problema: Se hoje é sexta-feira, que dia da semana será daqui a 1520 dias?

Para organizar o raciocínio, indiquemos por 0 o dia de hoje (sexta-feira), por 1 o dia de amanhã (sábado), e assim por diante. A partir dessa escolha, podemos construir o seguinte quadro:

Sexta	Sábado	Domingo	Segunda	Terça	Quarta	Quinta
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
...	...	...	...	...	....	...

Com essa tabela podemos perceber que 0= 7= 14 e assim por diante. Nossa questão se resume em saber em que coluna da tabela se encontra o número 1520. Para isso basta observar que dois números da sequência 0, 1, 2, 3, ... estão na mesma coluna se, e somente se, sua diferença é diferença é divisível por 7. Suponhamos que o numero 1520 se encontre na coluna encabeçada pelo número a $(0 \leq a \leq 6)$. Então, $1520 - a = 7q$, para algum inteiro positivo q. Daí $1520 = 7q + a$, $(0 \leq a \leq 6)$. Ora a unicidade do resto na divisão euclidiana, segue dessa igualdade que a é o resto da divisão de 1520 por 7. Observando que: $1520 = (7 \times 217) + 1$. Conclui-se que esse resto é 1 e que, portanto, 1520 está na segunda coluna. Logo daqui a 1520 dias será um sábado.

A tabela a seguir será importante para o aluno visualizar que a letra A é correspondente a infinitos números: 0, 26, 52, 78....

A	0	26	52	78	104
B	1	27	53	79	105
C	2	28	54	80	106
D	3	29	55	81	107
E	4	30	56	82	108
F	5	31	57	83	109
G	6	32	58	84	110
H	7	33	59	85	111
I	8	34	60	86	112
J	9	35	61	87	113
K	10	36	62	88	114
L	11	37	63	89	115
M	12	38	64	90	116
N	13	39	65	91	117
O	14	40	66	92	118
P	15	41	67	93	119
Q	16	42	68	94	120
R	17	43	69	95	121
S	18	44	70	96	122
T	19	45	71	97	123
U	20	46	72	98	124
V	21	47	73	99	125
W	22	48	74	100	126
X	23	49	75	101	127
Y	24	50	76	102	128
Z	25	51	77	103	129

A	130	156	182	208	234
B	131	157	183	209	235
C	132	158	184	210	236
D	133	159	185	211	237
E	134	160	186	212	238
F	135	161	187	213	239
G	136	162	188	214	240
H	137	163	189	215	241
I	138	164	190	216	242
J	139	165	191	217	243
K	140	166	192	218	244
L	141	167	193	219	245
M	142	168	194	220	246
N	143	169	195	221	247
O	144	170	196	222	248
P	145	171	197	223	249
Q	146	172	198	224	250
R	147	173	199	225	251
S	148	174	200	226	252
T	149	175	201	227	253
U	150	176	202	228	254
V	151	177	203	229	255
W	152	178	204	230	256
X	153	179	205	231	257
Y	154	180	206	232	258
Z	155	181	207	233	259

A	260	286	312	338	364
B	261	287	313	339	365
C	262	288	314	340	366
D	263	289	315	341	367
E	264	290	316	342	368
F	265	291	317	343	369
G	266	292	318	344	370
H	267	293	319	345	371
I	268	294	320	346	372
J	269	295	321	347	373
K	270	296	322	348	374
L	271	297	323	349	375
M	272	298	324	350	376
N	273	299	325	351	377
O	274	300	326	352	378
P	275	301	327	353	379
Q	276	302	328	354	380
R	277	303	329	355	381
S	278	304	330	356	382
T	279	305	331	357	383
U	280	306	332	358	384
V	281	307	333	359	385
W	282	308	334	360	386
X	283	309	335	361	387
Y	284	310	336	362	388
Z	285	311	337	363	389

Para realizarmos essa atividade podemos utilizar o recurso disponível em uma planilha eletrônica, pois facilita os cálculos.

Nas tabelas a seguir o * sempre indicará o resto da divisão por 26.

Com isso sabemos que não importa o valor do b, o que define como o alfabeto ficará é o valor do a.

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

$3x$	*	
0	0	A
3	3	D
6	6	G
9	9	J
12	12	M
15	15	P
18	18	S
21	21	V
24	24	Y
27	1	B
30	4	E
33	7	H
36	10	K
39	13	N
42	16	Q
45	19	T
48	22	W
51	25	Z
54	2	C
57	5	F
60	8	I
63	11	L
66	14	O
69	17	R
72	20	U
75	23	X

$3x+1$	*	
1	1	B
4	4	E
7	7	H
10	10	K
13	13	N
16	16	Q
19	19	T
22	22	W
25	25	Z
28	2	C
31	5	F
34	8	I
37	11	L
40	14	O
43	17	R
46	20	U
49	23	X
52	0	A
55	3	D
58	6	G
61	9	J
64	12	M
67	15	P
70	18	S
73	21	V
76	24	Y

$3x+2$	*	
2	2	C
5	5	F
8	8	I
11	11	L
14	14	O
17	17	R
20	20	U
23	23	X
26	0	A
29	3	D
32	6	G
35	9	J
38	12	M
41	15	P
44	18	S
47	21	V
50	24	Y
53	1	B
56	4	E
59	7	H
62	10	K
65	13	N
68	16	Q
71	19	T
74	22	W
77	25	Z

$3x+3$	*	
3	3	D
6	6	G
9	9	J
12	12	M
15	15	P
18	18	S
21	21	V
24	24	Y
27	1	B
30	4	E
33	7	H
36	10	K
39	13	N
42	16	Q
45	19	T
48	22	W
51	25	Z
54	2	C
57	5	F
60	8	I
63	11	L
66	14	O
69	17	R
72	20	U
75	23	X
78	0	A

Podemos construir os discos de criptografar com a sequência $(3a + b)$, pois percebemos que independente do b as letras sempre estarão nessa ordem:

Percebemos que quando multiplicamos o numero por 3 por exemplo, não importa o número que se soma. A sequência de letras obtidas sempre será a mesma.

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

* $3x \ mod \ 26$ (resto da divisão por 26)

Portanto podemos construir um disco para as transformações da forma $3a + b$.

Faremos o mesmo para $(2a + b)$, $(4a + b)$ e com $(6a + b)$

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

$2x$	*	
0	0	A
2	2	C
4	4	E
6	6	G
8	8	I
10	10	K
12	12	M
14	14	O
16	16	Q
18	18	S
20	20	U
22	22	W
24	24	Y
26	0	A
28	2	C
30	4	E
32	6	G
34	8	I
36	10	K
38	12	M
40	14	O
42	16	Q
44	18	S
46	20	U
48	22	W
50	24	Y

$4x$	*	
0	0	A
4	4	E
8	8	I
12	12	M
16	16	Q
20	20	U
24	24	Y
28	2	C
32	6	G
36	10	K
40	14	O
44	18	S
48	22	W
52	0	A
56	4	E
60	8	I
64	12	M
68	16	Q
72	20	U
76	24	Y
80	2	C
84	6	G
88	10	K
92	14	O
96	18	S
100	22	W

$6x$	*	
0	0	A
6	6	G
12	12	M
18	18	S
24	24	Y
30	4	E
36	10	K
42	16	Q
48	22	W
54	2	C
60	8	I
66	14	O
72	20	U
78	0	A
84	6	G
90	12	M
96	18	S
102	24	Y
108	4	E
114	10	K
120	16	Q
126	22	W
132	2	C
138	8	I
144	14	O
150	20	U

- $(2a + b)$

A	C	E	G	I	K	M	O	Q	S	U	W	Y	A	C	E	G	I	K	M	O	Q	S	U	W	Y

- $(4a + b)$

A	E	I	M	Q	U	Y	C	G	K	O	S	W	A	E	I	M	Q	U	Y	C	G	K	O	S	W

- $(6a + b)$

A	G	M	S	Y	E	K	Q	W	C	I	O	U	A	G	M	S	Y	E	K	Q	W	C	I	O	U

Percebemos que com $(2a + b)$, $(4a + b)$ e $(6a + b)$ não é possível se criptografar mensagens pois temos duas letras levando ao mesmo resultado, sendo impossível voltar a mensagem original.

Observando agora para $(5a + b)$ e $(7a + b)$

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

$5x$	*	
0	0	A
5	5	F
10	10	K
15	15	P
20	20	U
25	25	Z
30	4	E
35	9	J
40	14	O
45	19	T
50	24	Y
55	3	D
60	8	I
65	13	N
70	18	S
75	23	X
80	2	C
85	7	H
90	12	M
95	17	R
100	22	W
105	1	B
110	6	G
115	11	L
120	16	Q
125	21	V

$5x + 1$	*	
1	1	B
6	6	G
11	11	L
16	16	Q
21	21	V
26	0	A
31	5	F
36	10	K
41	15	P
46	20	U
51	25	Z
56	4	E
61	9	J
66	14	O
71	19	T
76	24	Y
81	3	D
86	8	I
91	13	N
96	18	S
101	23	X
106	2	C
111	7	H
116	12	M
121	17	R
126	22	W

$5x + 2$	*	
2	2	C
7	7	H
12	12	M
17	17	R
22	22	W
27	1	B
32	6	G
37	11	L
42	16	Q
47	21	V
52	0	A
57	5	F
62	10	K
67	15	P
72	20	U
77	25	Z
82	4	E
87	9	J
92	14	O
97	19	T
102	24	Y
107	3	D
112	8	I
117	13	N
122	18	S
127	23	X

$5x + 3$	*	
3	3	D
8	8	I
13	13	N
18	18	S
23	23	X
28	2	C
33	7	H
38	12	M
43	17	R
48	22	W
53	1	B
58	6	G
63	11	L
68	16	Q
73	21	V
78	0	A
83	5	F
88	10	K
93	15	P
98	20	U
103	25	Z
108	4	E
113	9	J
118	14	O
123	19	T
128	24	Y

- $(5a + b)$

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

- $(7a + b)$

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

Com a multiplicação pelas constates 5 e 7 percebemos que será possível criptografar mensagens pois temos que letras diferentes levam em letras diferentes.

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

$7x$	*	
0	0	A
7	7	H
14	14	O
21	21	V
28	2	C
35	9	J
42	16	Q
49	23	X
56	4	E
63	11	L
70	18	S
77	25	Z
84	6	G
91	13	N
98	20	U
105	1	B
112	8	I
119	15	P
126	22	W
133	3	D
140	10	K
147	17	R
154	24	Y
161	5	F
168	12	M
175	19	T

$7x+1$	*	
1	1	B
8	8	I
15	15	P
22	22	W
29	3	D
36	10	K
43	17	R
50	24	Y
57	5	F
64	12	M
71	19	T
78	0	A
85	7	H
92	14	O
99	21	V
106	2	C
113	9	J
120	16	Q
127	23	X
134	4	E
141	11	L
148	18	S
155	25	Z
162	6	G
169	13	N
176	20	U

$7x+2$	*	
2	2	C
9	9	J
16	16	Q
23	23	X
30	4	E
37	11	L
44	18	S
51	25	Z
58	6	G
65	13	N
72	20	U
79	1	B
86	8	I
93	15	P
100	22	W
107	3	D
114	10	K
121	17	R
128	24	Y
135	5	F
142	12	M
149	19	T
156	0	A
163	7	H
170	14	O
177	21	V

$7x+3$	*	
3	3	D
10	10	K
17	17	R
24	24	Y
31	5	F
38	12	M
45	19	T
52	0	A
59	7	H
66	14	O
73	21	V
80	2	C
87	9	J
94	16	Q
101	23	X
108	4	E
115	11	L
122	18	S
129	25	Z
136	6	G
143	13	N
150	20	U
157	1	B
164	8	I
171	15	P
178	22	W

Observemos o resultado para $(8a + b)$, $(10a + b)$ e $(12a + b)$.

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

$8x$	*	
0	0	A
8	8	I
16	16	Q
24	24	Y
32	6	G
40	14	O
48	22	W
56	4	E
64	12	M
72	20	U
80	2	C
88	10	K
96	18	S
104	0	A
112	8	I
120	16	Q
128	24	Y
136	6	G
144	14	O
152	22	W
160	4	E
168	12	M
176	20	U
184	2	C
192	10	K
200	18	S

$10x$	*	
0	0	A
10	10	K
20	20	U
30	4	E
40	14	O
50	24	Y
60	8	I
70	18	S
80	2	C
90	12	M
100	22	W
110	6	G
120	16	Q
130	0	A
140	10	K
150	20	U
160	4	E
170	14	O
180	24	Y
190	8	I
200	18	S
210	2	C
220	12	M
230	22	W
240	6	G
250	16	Q

$12x$	*	
0	0	A
12	12	M
24	24	Y
36	10	K
48	22	W
60	8	I
72	20	U
84	6	G
96	18	S
108	4	E
120	16	Q
132	2	C
144	14	O
156	0	A
168	12	M
180	24	Y
192	10	K
204	22	W
216	8	I
228	20	U
240	6	G
252	18	S
264	4	E
276	16	Q
288	2	C
300	14	O

- $(8a + b)$

A	I	Q	Y	G	O	W	E	M	U	C	K	S	A	I	Q	Y	G	O	W	E	M	U	C	K	S

- $(10a + b)$

A	K	U	E	O	Y	I	S	C	M	W	G	Q	A	K	U	E	O	Y	I	S	C	M	W	G	Q

- $(12a + b)$

A	M	Y	K	W	I	U	G	S	E	Q	C	O	A	M	Y	K	W	I	U	G	S	E	Q	C	O

Com as constantes 8, 10 e 12 não será possível criptografar pois temos duas letras diferentes levando ao mesmo resultado.

Agora observemos para $(9a + b)$

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

$9x$	*	
0	0	A
9	9	J
18	18	S
27	1	B
36	10	K
45	19	T
54	2	C
63	11	L
72	20	U
81	3	D
90	12	M
99	21	V
108	4	E
117	13	N
126	22	W
135	5	F
144	14	O
153	23	X
162	6	G
171	15	P
180	24	Y
189	7	H
198	16	Q
207	25	Z
216	8	I
225	17	R

$9x + 1$	*	
1	1	B
10	10	K
19	19	T
28	2	C
37	11	L
46	20	U
55	3	D
64	12	M
73	21	V
82	4	E
91	13	N
100	22	W
109	5	F
118	14	O
127	23	X
136	6	G
145	15	P
154	24	Y
163	7	H
172	16	Q
181	25	Z
190	8	I
199	17	R
208	0	A
217	9	J
226	18	S

$9x + 2$	*	
2	2	C
11	11	L
20	20	U
29	3	D
38	12	M
47	21	V
56	4	E
65	13	N
74	22	W
83	5	F
92	14	O
101	23	X
110	6	G
119	15	P
128	24	Y
137	7	H
146	16	Q
155	25	Z
164	8	I
173	17	R
182	0	A
191	9	J
200	18	S
209	1	B
218	10	K
227	19	T

$9x + 3$	*	
3	3	D
12	12	M
21	21	V
30	4	E
39	13	N
48	22	W
57	5	F
66	14	O
75	23	X
84	6	G
93	15	P
102	24	Y
111	7	H
120	16	Q
129	25	Z
138	8	I
147	17	R
156	0	A
165	9	J
174	18	S
183	1	B
192	10	K
201	19	T
210	2	C
219	11	L
228	20	U

- $(9a + b)$

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

Com a constate 9 temos sempre letras diferentes em letras diferentes.

Até esse momento podemos perceber que a possibilidade de criptografar acontece quando multiplicamos o número por um algarismo ímpar e não possibilidade quando multiplicamos por um número par.

Então diante dessa possibilidade iremos fazer a multiplicação por 13, ou seja da forma $(13a + b)$.

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

$13x$	*	
0	0	A
13	13	N
26	0	A
39	13	N
52	0	A
65	13	N
78	0	A
91	13	N
104	0	A
117	13	N
130	0	A
143	13	N
156	0	A
169	13	N
182	0	A
195	13	N
208	0	A
221	13	N
234	0	A
247	13	N
260	0	A
273	13	N
286	0	A
299	13	N
312	0	A
325	13	N

- $(13a + b)$

A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N	A	N

Portanto não é quando um número é impar que temos a possibilidade da multiplicação, pois 13 é impar e mesmo assim letras diferentes levam em letras iguais.

Agora faremos com os números 14, 16, 18 e 20

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

$14x$	*	
0	0	A
14	14	O
28	2	C
42	16	Q
56	4	E
70	18	S
84	6	G
98	20	U
112	8	I
126	22	W
140	10	K
154	24	Y
168	12	M
182	0	A
196	14	O
210	2	C
224	16	Q
238	4	E
252	18	S
266	6	G
280	20	U
294	8	I
308	22	W
322	10	K
336	24	Y
350	12	M

$16x$	*	
0	0	A
16	16	Q
32	6	G
48	22	W
64	12	M
80	2	C
96	18	S
112	8	I
128	24	Y
144	14	O
160	4	E
176	20	U
192	10	K
208	0	A
224	16	Q
240	6	G
256	22	W
272	12	M
288	2	C
304	18	S
320	8	I
336	24	Y
352	14	O
368	4	E
384	20	U
400	10	K

$18x$	*	
0	0	A
18	18	S
36	10	K
54	2	C
72	20	U
90	12	M
108	4	E
126	22	W
144	14	O
162	6	G
180	24	Y
198	16	Q
216	8	I
234	0	A
252	18	S
270	10	K
288	2	C
306	20	U
324	12	M
342	4	E
360	22	W
378	14	O
396	6	G
414	24	Y
432	16	Q
450	8	I

$20x$	*	
0	0	A
20	20	U
40	14	O
60	8	I
80	2	C
100	22	W
120	16	Q
140	10	K
160	4	E
180	24	Y
200	18	S
220	12	M
240	6	G
260	0	A
280	20	U
300	14	O
320	8	I
340	2	C
360	22	W
380	16	Q
400	10	K
420	4	E
440	24	Y
460	18	S
480	12	M
500	6	G

- $(14a + b)$

A	O	C	Q	E	S	G	U	I	W	K	Y	M	A	O	C	Q	E	S	G	U	I	W	K	Y	M

- $(16a + b)$

A	Q	G	W	M	C	S	I	Y	O	E	U	K	A	Q	G	W	M	C	S	I	Y	O	E	U	K

- $(18a + b)$

A	S	K	C	U	M	E	W	O	G	Y	Q	I	A	S	K	C	U	M	E	W	O	G	Y	A	I

- $(20a + b)$

A	U	O	I	C	W	Q	K	E	Y	S	M	G	A	U	O	I	C	W	Q	K	E	Y	S	M	G

Verificando para $(15a + b)$, temos:

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

$15x$	*	
0	0	A
15	15	P
30	4	E
45	19	T
60	8	I
75	23	X
90	12	M
105	1	B
120	16	Q
135	5	F
150	20	U
165	9	J
180	24	Y
195	12	M
210	2	C
225	17	R
240	6	G
255	21	V
270	10	K
285	25	Z
300	14	O
315	3	D
330	18	S
345	7	H
360	22	W
375	11	L

$15x + 1$	*	
1	1	B
16	16	Q
31	5	F
46	20	U
61	9	J
76	24	Y
91	12	M
106	2	C
121	17	R
136	6	G
151	21	V
166	10	K
181	25	Z
196	14	O
211	3	D
226	18	S
241	7	H
256	22	W
271	11	L
286	0	A
301	15	P
316	4	E
331	19	T
346	8	I
361	23	X
376	12	M

$15x + 2$	*	
2	2	C
17	17	R
32	6	G
47	21	V
62	10	K
77	25	Z
92	14	O
107	3	D
122	18	S
137	7	H
152	22	W
167	11	L
182	0	A
197	15	P
212	4	E
227	19	T
242	8	I
257	23	X
272	12	M
287	1	B
302	16	Q
317	5	F
332	20	U
347	9	J
362	24	Y
377	12	M

$15x + 3$	*	
3	3	D
18	18	S
33	7	H
48	22	W
63	11	L
78	0	A
93	15	P
108	4	E
123	19	T
138	8	I
153	23	X
168	12	M
183	1	B
198	16	Q
213	5	F
228	20	U
243	9	J
258	24	Y
273	12	M
288	2	C
303	17	R
318	6	G
333	21	V
348	10	K
363	25	Z
378	14	O

- $(15a + b)$

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

- Para $(17a + b)$

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

$17x$	*	
0	0	A
17	17	R
34	8	I
51	25	Z
68	16	Q
85	7	H
102	24	Y
119	15	P
136	6	G
153	23	X
170	14	O
187	5	F
204	22	W
221	13	N
238	4	E
255	21	V
272	12	M
289	3	D
306	20	U
323	11	L
340	2	C
357	19	T
374	10	K
391	1	B
408	18	S
425	9	J

$17x + 1$	*	
1	1	B
18	18	S
35	9	J
52	0	A
69	17	R
86	8	I
103	25	Z
120	16	Q
137	7	H
154	24	Y
171	15	P
188	6	G
205	23	X
222	14	O
239	5	F
256	22	W
273	13	N
290	4	E
307	21	V
324	12	M
341	3	D
358	20	U
375	11	L
392	2	C
409	19	T
426	10	K

$17x + 2$	*	
2	2	C
19	19	T
36	10	K
53	1	B
70	18	S
87	9	J
104	0	A
121	17	R
138	8	I
155	25	Z
172	16	Q
189	7	H
206	24	Y
223	15	P
240	6	G
257	23	X
274	14	O
291	5	F
308	22	W
325	13	N
342	4	E
359	21	V
376	12	M
393	3	D
410	20	U
427	11	L

$17x + 3$	*	
3	3	D
20	20	U
37	11	L
54	2	C
71	19	T
88	10	K
105	1	B
122	18	S
139	9	J
156	0	A
173	17	R
190	8	I
207	25	Z
224	16	Q
241	7	H
258	24	Y
275	15	P
292	6	G
309	23	X
326	14	O
343	5	F
360	22	W
377	13	N
394	4	E
411	21	V
428	12	M

- $(17a + b)$

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

Para $(19a + b)$

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

$19x$	*	
0	0	A
19	19	T
38	12	M
57	5	F
76	24	Y
95	17	R
114	10	K
133	3	D
152	22	W
171	15	P
190	8	I
209	1	B
228	20	U
247	13	N
266	6	G
285	25	Z
304	18	S
323	11	L
342	4	E
361	23	X
380	16	Q
399	9	J
418	2	C
437	21	V
456	14	O
475	7	H

$19x + 1$	*	
1	1	B
20	20	U
39	13	N
58	6	G
77	25	Z
96	18	S
115	11	L
134	4	E
153	23	X
172	16	Q
191	9	J
210	2	C
229	21	V
248	14	O
267	7	H
286	0	A
305	19	T
324	12	M
343	5	F
362	24	Y
381	17	R
400	10	K
419	3	D
438	22	W
457	15	P
476	8	I

$19x + 2$	*	
2	2	C
21	21	V
40	14	O
59	7	H
78	0	A
97	19	T
116	12	M
135	5	F
154	24	Y
173	17	R
192	10	K
211	3	D
230	22	W
249	15	P
268	8	I
287	1	B
306	20	U
325	13	N
344	6	G
363	25	Z
382	18	S
401	11	L
420	4	E
439	23	X
458	16	Q
477	9	J

$19x + 3$	*	
3	3	D
22	22	W
41	15	P
60	8	I
79	1	B
98	20	U
117	13	N
136	6	G
155	25	Z
174	18	S
193	11	L
212	4	E
231	23	X
250	16	Q
269	9	J
288	2	C
307	21	V
326	14	O
345	7	H
364	0	A
383	19	T
402	12	M
421	5	F
440	24	Y
459	17	R
478	10	K

- $(19a + b)$

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

.

Para $(21a + b)$

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

$21x$	*	
0	0	A
21	21	V
42	16	Q
63	11	L
84	6	G
105	1	B
126	22	W
147	17	R
168	12	M
189	7	H
210	2	C
231	23	X
252	18	S
273	13	N
294	8	I
315	3	D
336	24	Y
357	19	T
378	14	O
399	9	J
420	4	E
441	25	Z
462	20	U
483	15	P
504	10	K
525	5	F

$21x + 1$	*	
1	1	B
22	22	W
43	17	R
64	12	M
85	7	H
106	2	C
127	23	X
148	18	S
169	13	N
190	8	I
211	3	D
232	24	Y
253	19	T
274	14	O
295	9	J
316	4	E
337	25	Z
358	20	U
379	15	P
400	10	K
421	5	F
442	0	A
463	21	V
484	16	Q
505	11	L
526	6	G

$21x + 2$	*	
2	2	C
23	23	X
44	18	S
65	13	N
86	8	I
107	3	D
128	24	Y
149	19	T
170	14	O
191	9	J
212	4	E
233	25	Z
254	20	U
275	15	P
296	10	K
317	5	F
338	0	A
359	21	V
380	16	Q
401	11	L
422	6	G
443	1	B
464	22	W
485	17	R
506	12	M
527	7	H

$21x + 3$	*	
3	3	D
24	24	Y
45	19	T
66	14	O
87	9	J
108	4	E
129	25	Z
150	20	U
171	15	P
192	10	K
213	5	F
234	0	A
255	21	V
276	16	Q
297	11	L
318	6	G
339	1	B
360	22	W
381	17	R
402	12	M
423	7	H
444	2	C
465	23	X
486	18	S
507	13	N
528	8	I

- $(21 * a + b)$

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

Agora faremos com os números 22, 24, 26.

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

$22x$	*	
0	0	A
22	22	W
44	18	S
66	14	O
88	10	K
110	6	G
132	2	C
154	24	Y
176	20	U
198	16	Q
220	12	M
242	8	I
264	4	E
286	0	A
308	22	W
330	18	S
352	14	O
374	10	K
396	6	G
418	2	C
440	24	Y
462	20	U
484	16	Q
506	12	M
528	8	I
550	4	E

$24x$	*	
0	0	A
24	24	Y
48	22	W
72	20	U
96	18	S
120	16	Q
144	14	O
168	12	M
192	10	K
216	8	I
240	6	G
264	4	E
288	2	C
312	0	A
336	24	Y
360	22	W
384	20	U
408	18	S
432	16	Q
456	14	O
480	12	M
504	10	K
528	8	I
552	6	G
576	4	E
600	2	C

$26x$	*	
0	0	A
26	0	A
52	0	A
78	0	A
104	0	A
130	0	A
156	0	A
182	0	A
208	0	A
234	0	A
260	0	A
286	0	A
312	0	A
338	0	A
364	0	A
390	0	A
416	0	A
442	0	A
468	0	A
494	0	A
520	0	A
546	0	A
572	0	A
598	0	A
624	0	A
650	0	A

- $(22a + b)$

A	W	S	O	K	G	C	Y	U	Q	M	I	E	A	W	S	O	K	G	C	Y	U	Q	M	I	E

- $(24a + b)$

A	Y	W	U	S	Q	O	M	K	I	G	E	C	A	Y	W	U	S	Q	O	M	K	I	G	E	C

- $(26a + b)$

A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A

$(23a + b)$

	x	$23x$	*	
A	0	0	0	A
B	1	23	23	X
C	2	46	20	U
D	3	69	17	R
E	4	92	14	O
F	5	115	11	L
G	6	138	8	I
H	7	161	5	F
I	8	184	2	C
J	9	207	25	Z
K	10	230	22	W
L	11	253	19	T
M	12	276	16	Q
N	13	299	13	N
O	14	322	10	K
P	15	345	7	H
Q	16	368	4	E
R	17	391	1	B
S	18	414	24	Y
T	19	437	21	V
U	20	460	18	S
V	21	483	15	P
W	22	506	12	M
X	23	529	9	J
Y	24	552	6	G
Z	25	575	3	D

$23x + 1$	*	
1	1	B
24	24	Y
47	21	V
70	18	S
93	15	P
116	12	M
139	9	J
162	6	G
185	3	D
208	0	A
231	23	X
254	20	U
277	17	R
300	14	O
323	11	L
346	8	I
369	5	F
392	2	C
415	25	Z
438	22	W
461	19	T
484	16	Q
507	13	N
530	10	K
553	7	H
576	4	E

$23x + 2$	*	
2	2	C
25	25	Z
48	22	W
71	19	T
94	16	Q
117	13	N
140	10	K
163	7	H
186	4	E
209	1	B
232	24	Y
255	21	V
278	18	S
301	15	P
324	12	M
347	9	J
370	6	G
393	3	D
416	0	A
439	23	X
462	20	U
485	17	R
508	14	O
531	11	L
554	8	I
577	5	F

$23x + 3$	*	
3	3	D
26	0	A
49	23	X
72	20	U
95	17	R
118	14	O
141	11	L
164	8	I
187	5	F
210	2	C
233	25	Z
256	22	W
279	19	T
302	16	Q
325	13	N
348	10	K
371	7	H
394	4	E
417	1	B
440	24	Y
463	21	V
486	18	S
509	15	P
532	12	M
555	9	J
578	6	G

- $(23a + b)$

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

$(25a + b)$

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

$25x$	*	
0	0	A
25	25	Z
50	24	Y
75	23	X
100	22	W
125	21	V
150	20	U
175	19	T
200	18	S
225	17	R
250	16	Q
275	15	P
300	14	O
325	13	N
350	12	M
375	11	L
400	10	K
425	9	J
450	8	I
475	7	H
500	6	G
525	5	F
550	4	E
575	3	D
600	2	C
625	1	B

$25x + 1$	*	
1	1	B
26	0	A
51	25	Z
76	24	Y
101	23	X
126	22	W
151	21	V
176	20	U
201	19	T
226	18	S
251	17	R
276	16	Q
301	15	P
326	14	O
351	13	N
376	12	M
401	11	L
426	10	K
451	9	J
476	8	I
501	7	H
526	6	G
551	5	F
576	4	E
601	3	D
626	2	C

$25x + 2$	*	
2	2	C
27	1	B
52	0	A
77	25	Z
102	24	Y
127	23	X
152	22	W
177	21	V
202	20	U
227	19	T
252	18	S
277	17	R
302	16	Q
327	15	P
352	14	O
377	13	N
402	12	M
427	11	L
452	10	K
477	9	J
502	8	I
527	7	H
552	6	G
577	5	F
602	4	E
627	3	D

$25x + 3$	*	
3	3	D
28	2	C
53	1	B
78	0	A
103	25	Z
128	24	Y
153	23	X
178	22	W
203	21	V
228	20	U
253	19	T
278	18	S
303	17	R
328	16	Q
353	15	P
378	14	O
403	13	N
428	12	M
453	11	L
478	10	K
503	9	J
528	8	I
553	7	H
578	6	G
603	5	F
628	4	E

- $(25a + b)$

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

Concluímos que os possíveis valores de a são: 3, 5, 7, 11, 15, 17, 19, 21, 23 e 25. Não podemos usar os valores: 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24.

Atividade 3.2.4 - Decriptografar mensagens usando a criptoanálise.

Analisando a música Aquarela temos a seguinte distribuição de frequência das letras.

Aquarela

Toquinho

Numa folha qualquer eu desenho um sol amarelo
E com cinco ou seis retas é fácil fazer um castelo
Corro o lápis em torno da mão e me dou uma luva
E se faço chover, com dois riscos tenho um guarda-chuva
Se um pinguinho de tinta cai num pedacinho azul do papel
Num instante imagino uma linda gaivota a voar no céu

Vai voando, contornando a imensa curva norte-sul
Vou com ela viajando Havaí, Pequim ou Istambul
Pinto um barco a vela branco navegando
É tanto céu e mar num beijo azul

Entre as nuvens vem surgindo um lindo avião rosa e grená
Tudo em volta colorindo, com suas luzes a piscar
Basta imaginar e ele está partindo, sereno e lindo
E se a gente quiser ele vai pousar

Numa folha qualquer eu desenho um navio de partida
Com alguns bons amigos bebendo de bem com a vida
De uma América a outra consigo passar num segundo
Giro um simples compasso e num círculo eu faço o mundo

Um menino caminha e caminhando chega no muro
E ali logo em frente a esperar pela gente o futuro está
E o futuro é uma astronave que tentamos pilotar
Não tem tempo nem piedade nem tem hora de chegar
Sem pedir licença muda nossa vida
Depois convida a rir ou chorar

Nessa estrada não nos cabe conhecer ou ver o que virá
O fim dela ninguém sabe bem ao certo onde vai dar

Vamos todos numa linda passarela
De uma aquarela que um dia enfim
Descolorirá

Numa folha qualquer eu desenho um sol amarelo
Que descolorirá
E com cinco ou seis retas é fácil fazer um castelo
Que descolorirá
Giro um simples compasso e num círculo eu faço o mundo
Que descolorirá.

	1ª E.	%	2ª E.	%	3ª E.	%	4ª E.	%	5ª E.	%	6ª E.	%	7ª E.	%	todas	%
A	31	**12,70**	21	**15,56**	18	**11,76**	19	**11,52**	26	**12,38**	23	**15,75**	14	**8,59**	152	**12,50**
B	0	**0,00**	4	**2,96**	1	**0,65**	4	**2,42**	0	**0,00**	3	**2,05**	0	**0,00**	12	**0,99**
C	14	**5,74**	6	**4,44**	3	**1,96**	8	**4,85**	8	**3,81**	5	**3,42**	12	**7,36**	56	**4,61**
D	9	**3,69**	4	**2,96**	6	**3,92**	9	**5,45**	9	**4,29**	9	**6,16**	5	**3,07**	51	**4,19**
E	24	**9,84**	10	**7,41**	22	**14,38**	15	**9,09**	31	**14,76**	19	**13,01**	20	**12,27**	141	**11,60**
F	4	**1,64**	0	**0,00**	0	**0,00**	2	**1,21**	3	**1,43**	2	**1,37**	4	**2,45**	15	**1,23**
G	4	**1,64**	1	**0,74**	4	**2,61**	5	**3,03**	4	**1,90**	1	**0,68**	1	**0,61**	20	**1,64**
H	7	**2,87**	1	**0,74**	0	**0,00**	2	**1,21**	6	**2,86**	1	**0,68**	2	**1,23**	19	**1,56**
I	16	**6,56**	8	**5,93**	11	**7,19**	9	**5,45**	11	**5,24**	8	**5,48**	9	**5,52**	72	**5,92**
J	0	**0,00**	2	**1,48**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	2	**0,16**
K	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**
L	11	**4,51**	5	**3,70**	7	**4,58**	5	**3,03**	5	**2,38**	5	**3,42**	11	**6,75**	49	**4,03**
M	16	**6,56**	7	**5,19**	5	**3,27**	14	**8,48**	15	**7,14**	8	**5,48**	10	**6,13**	75	**6,17**
N	16	**6,56**	13	**9,63**	12	**7,84**	11	**6,67**	16	**7,62**	10	**6,85**	5	**3,07**	83	**6,83**
O	28	**11,48**	16	**11,85**	14	**9,15**	19	**11,52**	21	**10,00**	14	**9,59**	21	**12,88**	133	**10,94**
P	5	**2,05**	2	**1,48**	3	**1,96**	4	**2,42**	7	**3,33**	1	**0,68**	2	**1,23**	24	**1,97**
Q	2	**0,82**	1	**0,74**	1	**0,65**	2	**1,21**	1	**0,48**	3	**2,05**	5	**3,07**	15	**1,23**
R	10	**4,10**	6	**4,44**	11	**7,19**	6	**3,64**	14	**6,67**	10	**6,85**	12	**7,36**	69	**5,67**
S	13	**5,33**	3	**2,22**	14	**9,15**	12	**7,27**	8	**3,81**	10	**6,85**	13	**7,98**	73	**6,00**
T	7	**2,87**	6	**4,44**	7	**4,58**	2	**1,21**	12	**5,71**	2	**1,37**	1	**0,61**	37	**3,04**
U	20	**8,20**	10	**7,41**	8	**5,23**	15	**9,09**	10	**4,76**	8	**5,48**	15	**9,20**	86	**7,07**
V	5	**2,05**	8	**5,93**	5	**3,27**	2	**1,21**	3	**1,43**	4	**2,74**	0	**0,00**	27	**2,22**
W	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**
X	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**
Y	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**	0	**0,00**
Z	2	**0,82**	1	**0,74**	1	**0,65**	0	**0,00**	0	**0,00**	0	**0,00**	1	**0,61**	5	**0,41**

Análise de frequência das letras do alfabeto na língua portuguesa é um método para decifrar mensagens criptografadas, pois geralmente as letras sempre aparecem com a mesma frequência nos textos em geral.

Frequência aproximada das letras em português.(Porcentagem)

A	B	C	D	E	F	G	H	I	J	K	L	M
14,6	1,0	3,8	4,9	12,5	1,0	1,3	1,2	6,1	0,4	0,02	2,7	4,7

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5,0	10,7	2,5	1,2	6,5	7,8	4,3	4,6	1,6	0,01	0,2	0,01	0,4

Os alunos analisarão o texto abaixo contando a frequência das letras do alfabeto.

CYKCBJC

Pkmc rsjxc ykcjykob ok loeopxs km esj cmcbbjs
O ism iapis sk eoae bohce ó rciaj rczob km icehojs
Isbbs s jcvae om hsbps lc mcs o mo lsk kMc jknc
O eo rcis ixsnob, ism lsae baeise hopxs km ukcblc ixknc
Eo km vapukapxs lo haphc ica pkm volciapxs czkj ls vcvoj
Pkm apehcpho amcuaps kMc janlc ucanshc c nscb os iok

Nca nscpls isphsbpcpls c amopec ikbnc psbho ekj
Nsk ism ojc nacdcpls xcnca voykam sk aehcmfkj
Vaphs km fcbis c nojc fbcpis pcnoucpls
O hcphs ioj o mcb pkm foads czkj

Ophbo CE pknope nom ekbuapls km japls cnacs bsec o ubopc
Hkls om nsjhc isjsbapls ism ekce jkzoe c vaeicb
Fcehc amcuapcb o ojo oehc vcbhapls eobops o japls
O eo c uopho ykaeob ojo nca vskecb

Pkmc rsjxc ykcjykob ok loeopxs km pcnas lo vcbhalc
Ism cjukpe fspe cmause fofopls lo fom ism c nalc
Lo kMc cmobaic c skhbc ispeaus vceecb pkm eoukpls
Uabs km ezmvjoe ismvcees o pkm iabikjs ok rcis s mkpls

Km mopaps icmapxc o icmapxcpls ixouc os mkbs
O cja jsus om rbopho c oevobcb vojc uopho s rkhkbs oehc
O s rkhkbs o kMc cehbspcno yko hophcmse vajshcb
Pcs hom homvs pom vaolclo pom hom xsbc lo ixoucb
Eom volab jaiopic mklc pseec nalc
Lovsze ispnalc c bab sk ixsbcb

Poeec oehbclc pcs pse icfo ispxoiob s knob s yko nabc
s ram lojc panukom ecfo fom cs iobhs splo nca lcb
Ncmse hslse pkmc japlc vceecbljc
Lo kMc cykcbljc yko km lac opram
loeisjsbabc

Pkmc rsjxc ykcjykob ok loeopxs km esj cmcbbjs
Yko loeisjsbabc
O ism iapis sk eoae bohce ó rciaj rczob km icehojs
Yko loeisjsbabc
Uabs km eamvjoe ismvcees o pkm iabikjs ok rcis s mkpls
Yko loeisjsbabc

Os alunos irão preencher essa tabela com a quantidade de vezes que cada letra aparece no texto cifrado acima

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

Observando a freqüência eles conseguirão descobrir as letras que mais aparecem e com algumas letras, consultarão os discos que eles possuem.

Com isso conseguirão saber qual a função que foi usada na encriptação do texto acima, pois eles terão em mãos todos os discos e automaticamente descobrindo-se algumas letras descobrirão qual a função foi usada.

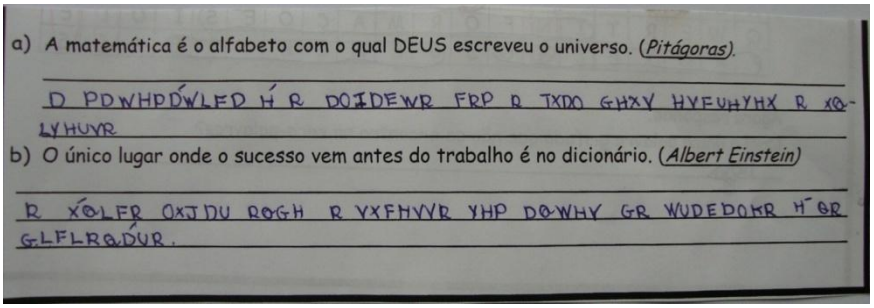
Capítulo 04- Prática

4.1- Atividade 1

A primeira atividade foi apresentada a história da Criptografia aos alunos. Iniciei perguntando se eles já haviam ouvido a palavra Criptografia, todos os alunos responderam que não conheciam esse termo. Falei que na nossa vida existem informações que não devem ser conhecidas de todas as pessoas. Existem informações que são pessoais. Por exemplo, o que aconteceria se todos conhecessem a senha do seu e-mail por exemplo. Eles falaram que não seria muito legal que outras pessoas vissem o seu e-mail. Com isso comentei que para proteger essas informações tem uma ciência chamada Criptografia, que nesse primeiro momento iríamos estudar como ela surgiu. Explique que ela surgiu na época das guerras, pois seus generais precisavam mandar mensagens secretas e seus inimigos não poderiam descobrir, pois era estratégia de guerra. Explique como a Cifra de César funcionava que era o deslocamento do alfabeto três posições a frente. Com isso escrevi o alfabeto na lousa e com eles perguntei: Se o alfabeto se desloca três posições a frente então o A vai ser? Todos responderam: D. E assim sucessivamente. Coloquei um exemplo na lousa, a palavra ALUNO, e vimos que se DOXQR. Falei que a Cifra de César não é mais utilizada hoje em dia, pois ela é de fácil decriptação, ou seja, é fácil de descobrir. Ficaram extremamente curiosos para saber como que funciona a encriptação de senhas hoje. Perguntaram insistentemente, queriam que a professora contasse o “segredo”, palavra deles, de como funciona hoje. Falei que não fazia parte do trabalho naquele momento. Acredito que eles imaginaram que se eu falasse como funcionam eles iriam conseguir descobrir todas as senhas existentes.

Para fazer as atividades de criptografar as duas frases e o caça palavras, os alunos levaram duas aulas de cinqüenta minutos. A maioria dos alunos compreendeu bem a atividade e conseguiram fazer tranquilamente as atividades. Foi muito produtiva, pois quase todos os alunos participaram, alguns tiveram dúvidas. Tem um aluno na sala que apresenta hiperatividade, ele só fez a atividade de caça- palavras e se recusou a fazer a outra, mesmo com explicação.

Percebi que depois alguns deles começaram a escrever bilhetes utilizando a Cifra de César.

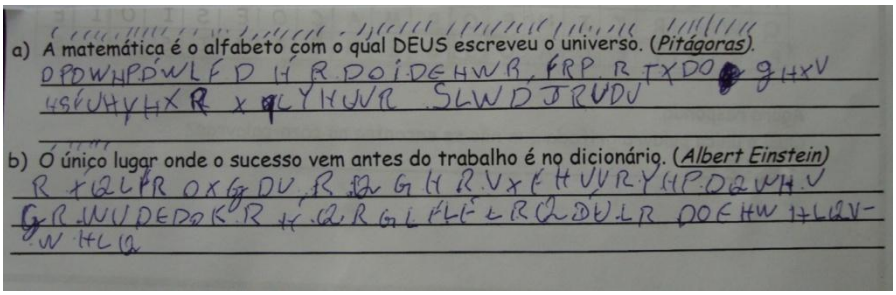

a) A matemática é o alfabeto com o qual DEUS escreveu o universo. (*Pitágoras*).

D PDWHPÁWLFD É R DOIDEWR FRP R TXDO GHXV HYEUHYHX R XQ-
LYHUYR

b) O único lugar onde o sucesso vem antes do trabalho é no dicionário. (*Albert Einstein*)

R XÓLFR OXJDU ROGH R YXFHYYR YHP DQWHV GR WUDEDOHR É GR
GLFLRQÁUR.

Figura 5- Resposta da atividade de um aluno do 7ºano.


a) A matemática é o alfabeto com o qual DEUS escreveu o universo. (*Pitágoras*).

DPDWHPÁWLFD É R DOÍDEHWR, FRP R TXDO GHXV
HVFUHYHX R XQLYHUVR. SLWDJRUDV

b) O único lugar onde o sucesso vem antes do trabalho é no dicionário. (*Albert Einstein*)

R ÚQLFR OXJDU, R GH R VXFHVVR YHP DQWHV
GR WUDEDOKR É R GLFLRQÁULR DOEHW 17LQV-
WLQ

Figura 6- Resposta da atividade de um aluno do 6º ano.

C	R	I	P	T	O	G	R	A	F	I	A	M	E	T	M	V	D	L	P
O	P	N	Y	R	T	U	E	W	Q	A	L	G	S	J	E	T	E	M	N
S	E	F	R	T	O	E	Z	N	H	T	F	I	T	P	N	P	S	W	A
S	W	O	N	M	Ã	R	P	L	J	H	A	A	R	W	S	N	T	B	D
W	D	R	T	Y	Ç	R	F	D	W	E	B	N	A	X	A	S	I	A	S
Z	X	M	B	X	I	A	L	H	C	O	E	Y	T	E	G	W	N	Y	S
S	T	A	T	R	U	E	X	V	O	N	T	N	É	O	E	P	A	L	J
W	E	Ç	R	Q	T	Ç	A	Ç	M	M	O	U	G	T	N	D	T	S	W
A	N	Õ	H	T	I	W	E	U	U	P	O	L	I	F	S	E	Á	R	V
Q	R	E	A	Q	T	E	V	R	N	H	J	Y	A	P	L	X	R	A	H
Z	E	S	P	I	S	T	E	A	I	B	D	E	S	S	Q	V	I	S	S
X	T	A	Q	X	B	N	N	C	C	W	Q	R	S	E	Y	U	O	É	P
Z	N	W	S	D	U	E	T	I	A	P	R	E	W	A	Q	X	Z	C	N
C	I	F	R	A	S	M	Q	N	Ç	B	V	X	Z	A	S	D	E	E	M
R	E	I	W	Q	P	A	D	U	Ã	L	F	A	B	E	T	O	T	D	S
S	Q	X	X	Z	B	G	Ç	M	O	R	T	Y	I	O	P	L	J	A	A
A	Q	O	V	B	M	I	X	O	A	Q	W	E	R	T	A	Q	A	R	H
A	S	Q	E	R	T	T	G	C	Ó	D	I	G	O	S	O	P	L	F	N
Q	W	E	R	T	I	N	F	O	R	M	A	Ç	Õ	E	S	I	O	I	E
P	R	O	T	E	Ç	Ã	O	S	G	E	N	E	R	A	I	S	A	C	S

Figura 7-Resposta da atividade de um aluno do 6º ano.

4.2 Atividade 2

Nessa atividade expliquei que podemos deslocar não somente três posições no alfabeto, mas que podemos deslocar quantas posições se desejar.

A sala foi dividida em seis grupos e cada grupo escolhia o deslocamento que preferir. Por exemplo, um dos grupos escolheu o deslocamento de doze posições a palavras ESCOLA se transformou em QEOAXM. Outro grupo escolheu o deslocamento de oito posições e a palavra MATEMÁTICA ficou assim: UIBMUIBQKI.

Depois que cada grupo encriptou sua palavra e não contou para o outro grupo a quantidade de deslocamento, os grupos trocaram as palavras e pelo preenchimento de todas as possibilidades de combinações foi possível a descoberta das palavras. Como por exemplo essas duas palavras:

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

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

Nessa atividade é possível a utilização do disco de criptografar que faz a correspondência de um disco menor em um disco maior concêntricos preenchidos com o alfabeto.

Essa atividade demorou duas aulas de cinqüenta minutos. Alguns alunos reclamaram que é muito trabalhoso se fazer a decriptação das palavras. Mas no geral gostaram da atividade e entenderam.

4.3- Atividade 3

Comecei essa atividade explicando que agora não iremos apenas deslocar posições a frente no alfabeto. Primeiramente iremos relacionar cada letra do alfabeto a um número, iniciando no zero e seguindo o vinte e cinco, pois são vinte e seis letras. Depois dessa relação iremos multiplicar cada número a uma constante. Percebemos que a partir de um valor o resultado se torna maior que 25. Expliquei que precisamos dividir o resultado por 26 e verificar o valor do resto. Pois como estamos trabalhando com o alfabeto que é um conjunto finito de 26 elementos, a partir dos 25 voltamos ao início novamente. Falei que podemos comparar com um relógio, pois quando o relógio indica 1 hora pode ser 1 hora ou 13 horas.

O exemplo utilizado para exemplificar na lousa foi da multiplicação. Primeiramente fiz a correspondência do alfabeto aos números. Multipliquei por 3 e depois fiz cada divisão com eles na lousa para verificar o resto. Montamos a nova seqüência de letras do alfabeto segundo a multiplicação por três.

Perguntei se cada letra tinha um correspondente diferente e eles perceberam que sim. Então disse que podemos criptografar utilizando a multiplicação por três.

Com essa parte da atividade foram gastos cinqüenta minutos, ou seja, uma aula.

Depois como próximos exemplos fizeram a multiplicação por dois. Seguindo o mesmo processo feito com três a partir do momento que o valor foi maior que 25, dividimos o valor por 26 e verificamos o resto. Com isso foi feita uma nova seqüência. Repeti a mesma pergunta em relação a multiplicação por 2 e eles chegaram a conclusão que tinham letras diferentes que apresentam o mesmo correspondente. Logo não era possível utilizar essa multiplicação para criptografar.

Fiz somente esses dois exemplos e já listei para eles quais são os valores que as multiplicações funcionam, ou seja, não tenho duas letras que se correspondem com uma mesma letra. Disse a eles que os valores que funcionam são: 3, 5, 7, 9, 11, 15, 17,19, 21, 23 e 25.

Mencionei que os valores que dão certo são aqueles que têm máximo divisor comum entre o número e vinte e seis iguais a um.

Apresentei os discos de criptografar, no caso um disco para cada valor que funciona.

4.4- Atividade 4

Nessa atividade iniciei com a explicação que as letras do alfabeto da língua portuguesa aparecem sempre com a mesma freqüência em qualquer texto, comentei que não podemos levar em conta quando são textos pequenos ou frases por exemplo. Mas no geral se estudarmos um texto que contenha um grande número de palavras as letras a freqüência das letras sempre será a mesma.

Apresentei a tabela de freqüência de letras do alfabeto aos alunos e disse quais letras aparecem com mais e quais aparecem menos.

Então falei que quando temos um texto criptografado podemos fazer uma contagem do número de letras, possivelmente aquela letra que aparecer mais será a letra A.

Propus que eles fizessem a contagem das letras do texto da atividade como tarefa para casa, mas a maioria dos alunos não fez isso. Então realizamos essa tarefa em outra aula. Uma dificuldade nessa atividade foi a concentração dos alunos, pois para a realização da contagem é necessário silêncio, o que não ocorreu, então os que estavam tentando contar se desconcentravam com facilidade, tornando a atividade de difícil realização.

Então simplesmente expliquei que quando descobrimos através da contagem qual as letras aparecem mais, podemos descobrir algumas letras e usando os discos podemos descobrir qual foi o número que usamos na multiplicação para a encriptação.

Capítulo 5 – Conclusões e Perspectivas

5.1 Conclusões

Atividades que busquem ligar o conteúdo de matemática com aplicações na vida cotidiana são interessantes para o aluno e também para o professor. Procurar fazer isso no dia a dia é um exercício que o professor precisa fazer.

A aprendizagem dos alunos está ligada a diversos fatores, um desses fatores é conteúdo estudado. Fazer com que o aluno se interesse por ele é um fator que só vem a contribuir para o aprendizado.

Minha primeira impressão quando fui apresentada ao tema Criptografia para o planejamento das atividades para alunos do sexto ano, alunos que possuem em média 11 anos, fiquei um tanto ansiosa quanto a dificuldade. Realmente não tinha a mínima idéia que seria possível realizar uma seqüência didática que se adequasse ao conteúdo e ao conhecimento prévio dos alunos desta faixa etária.

Na elaboração das atividades tive um pouco de dificuldades. Primeiramente me deparei com a falta de atividades relacionadas a Criptografia para o ensino fundamental, não temos disponibilizados material para pesquisa. Mas percebi que era possível, não com todo rigor matemático da formalização de uma função, mas usando as ferramentas que eles têm disponível.

Procurei elaborar atividades bem detalhadas, que todos os passos estejam bem escritos, essa idade não possui maturidade matemática para generalizar casos. Eles precisam ver caso por caso. Também usei uma ferramenta que facilita a realização das atividades, que é o disco de criptografar.

No momento que comecei a aplicar essas atividades em sala de aula tive uma surpresa muito positiva, pois os alunos do sexto ano se interessaram pelo tema e o melhor é que eles entenderam o conceito.

Nessas atividades usamos a Criptografia antiga, ou seja, essa criptografia não é mais utilizada hoje em dia. Mas esse tema desperta o interesse dos alunos em saber qual é a usada hoje em dia. Limitei-me a responder que hoje são os computadores que fazem isso e não é mais um processo manual. Mas realmente eles insistiram bastante perguntando como se fazia para decriptar mensagens hoje em dia, como senhas por exemplo. Com isso percebi que conhecendo como a Criptografia surgiu, faz com que os alunos fiquem mais curiosos para entender como ela funciona hoje.

Também tive dificuldades para a realização das atividades pela indisciplina de alguns alunos. A Escola está localizada na periferia de Dourados, a maioria dos alunos não tem apoio dos pais para a realização das tarefas para casa, pois a maioria trabalha o dia todo.

Não adianta enviar atividades para serem feitas em casa, pois na maioria das vezes não são realizadas. Todas as atividades devem ser realizadas em sala de aula.

Considerei que as atividades aplicadas apresentaram bons resultados que pude constatar através das reações de alguns, como comentários que era uma atividade legal. Também no envolvimento e questionamentos feitos pelos alunos.

No geral foi muito gratificante o trabalho realizado. Eles começaram a ver a matemática com um olhar diferente, ou seja, como eles mesmos dizem: “que serve para alguma coisa”. Me fez refletir sobre minha prática pedagógica e como podemos preparar uma aula mais elaborada.

5.2 – Perspectivas

Comecei a trabalhar como professora de matemática em 2005. Nunca tinha trabalhado com esse tema. Sempre segui a lista de conteúdos apresentados pelo livro didático e não tinha pensando a respeito de procurar atividades diferenciadas para aumentar o interesse do aluno pela matemática.

É trabalhoso sair da zona de conforto, pois precisamos fazer mais pesquisa e se gasta mais tempo para a preparação de aulas.

Comecei a pesquisar sobre esse tema e pude perceber que existem muitas possibilidades para se trabalhar atividades relacionadas com os conteúdos propostos para praticamente o ensino fundamental e médio.

Essas atividades são somente a parte inicial do Estudo da Criptografia. Conforme a idade escolar aumenta, as possibilidades de utilização desse tema aumentam. Então realmente considero que é um tema extremamente importante que podemos continuar o trabalho em anos finais do ensino fundamental e ensino médio.

Com isso pretendo continuar com a pesquisa referente a essa tema e buscar mais atividades relacionadas a ele. Dentro das possibilidades pretendo inserir a partir de agora no currículo das turmas esse tema, pois algumas escola são flexíveis quanto ao planejamento e as atividades propostas, outras não tem como mudar todo o planejamento.

Referências

B. FABIO ***Criptografia como Ferramenta para o Ensino de Matemática***. Disponível em: http://www.sbmac.org.br/eventos/cnmac/xxxi_cnmac/PDF/189.pdf

C. EDILSON ***A criptografia e seu papel na segurança da informação e das comunicações (sic) – retrospectiva, atualidade e perspectiva***. Disponível em: http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/edilson_fernandes.pdf

Vídeo disponível: http://www.youtube.com/watch?v=UoS8iJY-3Fo

FREIRE, P.; CASTILHO, J. E. ***A matemática dos códigos criptográficos***. Disponível em http://www.ucb.br/sites/100/103/TCC/12007/PalomaBarbosaFreire.pdf

L.MANOEL ***Criptografia, números e algoritmos***. Disponível em http://www.impa.br/opencms/pt/biblioteca/pm/PM_04.pdf

Q. PEDRO ***Criptografia***. Disponível em http://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia1011/artigo-gazeta08.pdf

DOURADOS, **Rede Municipal de Ensino de Dourados- MS. *Proposta Curricular da Educação Básica.* 2012**

FRANÇA, W.B.de A. ***Criptografia***. Disponível em: http://www.ucb.br/sites/100/103/TCC/22005/WaldizarBorgesdeAraujoFranco.pdf

SINGH, S. ***O livro dos códigos***. Rio de Janeiro. Record 2001

FRANCESE, J. P.S. ***Criptografia Quântica***. Disponível em: http://www.gta.ufrj.br/grad/08_1/quantica/dw/Criptografia%20Quantica%20(Joao%20Pedro%20Francese).doc

COUTINHO, S. C. ***Números Inteiros e Criptografia*** RSA. IMPA- SBM