UNIVERSIDADE FEDERAL DO TOCANTINS
CÂMPUS UNIVERSITÁRIO DE PALMAS
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL – PROFMAT

GILMAR REZENDE DE OLIVEIRA JÚNIOR

ALGUMAS APLICAÇÕES DA CRIPTOGRAFIA NO ENSINO FUNDAMENTAL

PALMAS - TO
2015

GILMAR REZENDE DE OLIVEIRA JÚNIOR

ALGUMAS APLICAÇÕES DA CRIPTOGRAFIA NO ENSINO FUNDAMENTAL

Trabalho de Conclusão de Curso apresentado ao programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para a obtenção do título de Mestre - Área de Concentração: Matemática. Orientador: Prof. Dr. Andrés Lázaro Barraza De La Cruz.

PALMAS - TO
2015

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

O48a Oliveira Junior, Gilmar Rezende de.

ALGUMAS APLICAÇÕES DA CRIPTOGRAFIA NO ENSINO FUNDAMENTAL. / Gilmar Rezende de Oliveira Junior. – Palmas, TO, 2015.

49 f.

Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado) Profissional em Matemática, 2015.

Orientador: Dr. Andrés Lázaro Barraza De La Cruz

1. Criptografia. 2. Ensino Fundamental. 3. Benefícios. 4. PCN. I. Título

CDD 510

GILMAR REZENDE DE OLIVEIRA JÚNIOR

ALGUMAS APLICAÇÕES DA CRIPTOGRAFIA NO ENSINO FUNDAMENTAL

Trabalho de Conclusão de Curso apresentado ao programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Tocantins como requisito parcial para obtenção do título de Mestre – Área de Concentração: Matemática.
Orientador: Dr. Andrés Lázaro Barraza De La Cruz.

Aprovada em 18 / 12 / 2015

BANCA EXAMINADORA

Andrés Barraza

Prof. Dr. Andrés Lázaro Barraza De La Cruz (UFT)

Rogério Azevedo Rocha

Prof. Dr. Rogério Azevedo Rocha (UFT))

Prof. Dr. Claudio de Castro Monteiro (IFTO)

À minha esposa Mariana Rezende.
Aos meus pais.
Aos meus amigos e colegas de mestrado.

Agradecimentos

À Deus, que sempre está iluminando meu caminho e me ajudando a conquistar vitórias.

À minha esposa e companheira Mariana, pelo carinho e paciência nesta etapa de nossa vida.

Aos familiares e amigos por todo o apoio e incentivo oferecidos nos bons e maus momentos.

À SBM (Sociedade Brasileira de Matemática) pela coordenação deste importante programa de mestrado.

À UFT (Universidade Federal do Tocantins) nas pessoas do professor coordenador Andrés Lázaro Barraza De La Cruz e dos professores Christian José Quintana Pinedo, Rogério Azevedo Rocha, Pedro Alexandre da Cruz, Gilmar Pires Novaes e Betty Clara Barraza De La Cruz pela significativa contribuição acadêmica.

Ao meu orientador, Profº Dr. Andrés Lázaro Barraza De La Cruz pela confiança depositada e conhecimentos transmitidos para a conclusão deste trabalho.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro.

Aos colegas de mestrado pelo convívio e amizade.

Aos colegas de trabalho pelo incentivo.

A todos os professores, sem os quais este momento não seria possível.

A mente que se abre a uma nova ideia
jamais voltará ao seu tamanho original
(Albert Einstein)

Resumo

Nesta dissertação foram mostradas através de pesquisas bibliográficas, situações problemas a aplicação da criptografia na sala de aula durante o ensino fundamental. A criptografia trata de ser a arte e ciência de fabricar códigos secretos. Assim, procura-se sempre a forma mais precisa de criação, além de ser o estudo das técnicas pelas quais uma informação pode ser modificada de forma a ficar oculta, ininteligível, salvo para o destinatário de direito da mensagem. Portanto a função da criptografia é de proteger uma informação. Dessa forma, os Parâmetros Curriculares Nacionais do Ensino Fundamental, a criptografia e sua historicidade, a criptografia artesanal, mecânica, digital e assimétrica, a inserção da criptográfica no currículo matemático e os seus benefícios, foram somente alguns dos tópicos apresentados nesse trabalho e que refletem diretamente a importância desse tema para a atualidade das salas de aula. Além disso, alguns exemplos da utilização da criptografia em sala de aula foram mostrados, principalmente pela necessidade de atingir o objetivo principal desse trabalho que consiste em descrever os benefícios da aplicação da criptografia no ensino fundamental para melhoria do aprendizado. E criado também um código fonte no software WxMáxima para o método RSA.

Palavras-chaves: Criptografia, Ensino Fundamental, Benefícios, PCN.

Abstract

In this thesis were shown, through bibliographic research, problems about the application of cryptography in the classroom during elementary school. Cryptography is the art and science of making secret codes. Thus, always demands the most accurate means of making, besides being the study of techniques by which information can be modified in order to stay hidden, unintelligible, except for who is the addressee. So, the role of cryptography is to protect information. The National Curricular Parameters for elementary school, cryptography and its historicity, handmade cryptography mechanics, digital and asymmetry, the insertion of cryptography in the mathematical curriculum and its benefits, were only some of the topics presented in this work and that directly reflect its importance for today's classrooms. Moreover, some examples of its using in classrooms were displayed, mainly by the need to achieve the major objective of this work, that is to describe the benefits of applying cryptography in elementary school for learning improvement. And also made a software source code xwMaxima for RSA process.

Key-words: Cryptography, Elementary School, Benefits, PCN.

Lista de ilustrações

Sumário

1 INTRODUÇÃO

A criptografia trata de ser a arte e ciência de fabricar códigos secretos. Assim, procura-se sempre a forma mais precisa de criação, além de ser o estudo das técnicas pelas quais uma informação pode ser modificada de forma a ficar oculta, ininteligível, salvo para o destinatário de direito da mensagem. Portanto a função da criptografia é de proteger uma informação. A palavra deriva do grego Kryptós,"escondido", e gráphein, "escrita". (FIGUEIREDO, 2012)

Como a informática está presente no cotidiano das pessoas de maneira muito intensa, acredita-se que o tema criptografia para os estudos de matemática podem se tornar bem mais interessantes, podendo funcionar como motivador para que os alunos possam sentir prazer em realizar exercícios e aprofundar temas desenvolvidos no ensino fundamental. E por meio dos professores levarem situações reais para dentro das salas de aula.

A Matemática é uma linguagem que pode ser expressa por meio de símbolos, números, palavras e enunciados de forma geral. Desse modo, compete abordar as dificuldades dos alunos que não conseguem compreender instruções e enunciados matemáticos, bem como as operações matemáticas (aritmética). Antes disso é necessário que eles superem as dificuldades relacionadas com a leitura, escrita (dislexia), coordenação motora (dispraxia) e outras para assim, acontecer à aprendizagem da matemática.

Com base no contexto relatado acima, este trabalho aborda o seguinte tema: "Algumas aplicações da criptografia no ensino fundamental", como forma de melhorar a assimilação dos conteúdos matemáticos dos alunos do ensino fundamental e consequentemente alterar a forma de trabalho do professor. O motivo pela escolha do tema foi perceber através da própria experiência profissional as dificuldades encontradas pelos alunos para assimilação dos conteúdos matemáticos.

Este trabalho é dividido em quatro capítulos No segundo capítulo é abordado os parâmetros curriculares nacionais do ensino fundamental assim como as dificuldades de aprendizagem da matemática e estratégias metodológicas para a melhoria do aprendizado. No terceiro capítulo é colocado as referências que se tem em criptografia, enfatizando seus fatos históricos e a evolução ao longo do tempo. No capítulo quatro é apresentado algumas sugestões de atividades para serem aplicadas em sala de aula na segunda fase do ensino fundamental (6^o ao 9^o ano), assim como abordagem do RSA por meio do software WxMáxima. Finalmente nas considerações finais é enfatizado a participação dos professores com aulas mais dinâmicas usando os recursos computacionais.

2 PARÂMETROS CURRICULARES NACIONAIS: ENSINO FUNDAMENTAL

O termo da escola deriva do latim schola e refere-se ao estabelecimento onde se dá qualquer gênero da instrução. Também permite fazer alusão ao ensino que se dá ou que se recebe ao conjunto do corpo docente e discente de um mesmo estabelecimento escolar, ao método, ao estilo peculiar de cada professor/docente para ensinar, à doutrina, aos princípios e ao sistema de um autor (PAROLIN, 2003).

No século XVII a escola surgiu como uma solução para muitos problemas, sendo considerada um suporte de apoio as famílias, uma espécie de complemento. Da mesma maneira que seus pais corriam até os comércios da época, para alimentar-se, vestir-se e comprar seus móveis, devia ter essa mesma disposição para encontrar escolas competentes na educação de seus filhos.

A matrícula das crianças na escola depende na maioria das vezes de seus pais, e isso se tornou natural que nem mesmo eles sabem a real razão ou a importância que isso significa.

Os pais, responsáveis pela educação do lar de suas crianças, não esperam da escola apenas a instrução de sala de aula, mas criam expectativas quanto seus valores morais, comportamento e princípios éticos.

> A escola, entretanto, tem uma especificidade, a obrigação de ensinar (bem) conteúdos específicos da área do saber, escolhidos como sendo fundamentais para a instrução de novas gerações. O problema de as crianças aprenderem fração é da escola. Família não tem nenhuma obrigação. Por outro lado, professora alguma tem de dar "carinho maternal" para seus alunos (SZYMANSKI, 2009, p. 99).

O carinho que a criança adquire no seu lar, é trabalhado pela família e a escola age apenas como parte complementar. Os valores morais e os princípios éticos são de inteira responsabilidade da família. A instituição conhecida como escola é que tem função de educar para a cidadania, aprimorar e desenvolver a maneira da criança viver em sociedade, e também aprender que nem todas as pessoas são iguais, lidando com as diferenças. O papel dos professores é adotar e alterar a visão das crianças com relação à escola, que elas voltem a ter o prazer e a felicidade de estudar e a cada dia lutar por um futuro melhor e mais digno.

A função da escola é ceder um espaço confiável para as crianças e que elas se sintam a vontade e protegidas naquele lugar e sempre em busca de um desenvolvimento conjunto. Nas instituições de ensino as crianças devem aprender a enfrentar desafios, passando

pelas tarefas didáticas individuais e em grupos, a monitoração e acompanhamento dos professores e isso é considerado tudo parte de um cronograma.

Um item que deve ser levado em consideração são as relações interpessoais, consistentes e precisas para melhorar o desenvolvimento das crianças, servindo mais ainda na sua adaptação com outras pessoas e com o espaço oferecido.

> É interessante observar que, em situações informais de aprendizado, as crianças costumam utilizar as interações sociais como forma privilegiada de acesso à informação: aprendem regras dos jogos, por exemplo, através dos outros e não como resultado de um empenho estritamente individual na solução de um problema. Qualquer modalidade de interação social, quando integrada num contexto realmente voltado para a promoção do aprendizado e do desenvolvimento, poderia ser utilizada, portanto, de forma produtiva na situação escolar (OLIVEIRA, 2005, p. 64).

A escola e a família devem ter uma parceria contínua e fortalecida, isso é fato. Mas se a escola não promover atividades que priorizem essa aproximação com a família, fica ainda mais difícil de mantê-las alicerçadas. Mas o que deve ser observado com relação a essa relação é que algumas famílias não sentem motivação e muita das vezes ainda se sentem inferiores a outras pessoas, principalmente na presença de outros pais, pelo fato de terem escolaridade inferior. No momento em que há alguma convocação de sua presença, ela acontece de maneira forçada o que gera uma situação extremamente embaraçosa.

> A família irá se sentir comprometida com a melhoria da qualidade escolar e com o desenvolvimento de seu filho como ser humano quando a escola oferecer oportunidades de contato para passar informações relevantes sobre seus objetivos, recursos, problemas e também sobre as questões pedagógicas (PARO, 1997, p. 67).

O conhecido Projeto Político Pedagógico (PPP) serve para facilitar a aproximação desses dois elementos, escola x família. Esse projeto tem como objetivo estabelecer uma linguagem mais fácil entre os dois, e o ponto positivo desse projeto é que ele passa de maneira clara os objetivos pedagógicos a serem alcançados e trabalhados durante todo o ano letivo.

É correto afirmar que o projeto pedagógico é uma proposta diferente com a intenção de suprir as necessidades da escola e constituir parâmetros reflexivos para um futuro promissor, no sentido de romper com o passado, implantado num cenário que é marcado pela variedade, e, nessa direção é que o projeto político pedagógico precisa ser feito com eficácia, participação e governo dentro de uma gestão democrática que proponha a descentralização dos métodos de tomada de decisão ampliando a autonomia escolar.

Diante disso, os PCN'S (Parâmetros Curriculares Nacionais) tratam do fator qualidade da educação, promovendo estratégias e ações voltadas para melhorar o ensino dos

alunos em todos os níveis. Todavia, a qualidade da atuação da escola não pode somente depender da vontade de um ou outro professor, muito pelo contrario é um conjunto de fatores e valores a que vem reger o ensino. Por isso, é indispensável à participação de todos os profissionais (orientadores, supervisores, professores polivalentes e especialistas) para que sejam tomadas as melhores decisões a respeito da prática didática, bem como sua execução. Ainda assim, é importante ressaltar que as decisões tomadas normalmente são bem diferentes, quando se trata de uma escola para outra, ou seja, o ambiente e a formação dos professores interferem bastante numa escolha ou decisão.

Dessa forma, para que o ensino seja de fato eficiente e gere os efeitos esperados é necessário que os profissionais estejam comprometidos, disponham de tempo e de recursos que atendam suas necessidades e dos seus alunos. Por outro lado, mesmo os professores e os alunos tendo excelentes condições de trabalho e de recursos, as dificuldades e limitações sempre estarão presentes, não há como estar preparado para todos os tipos de situações, pois na escola se manifestam os conflitos existentes na sociedade.

> As considerações feitas pretendem auxiliar os professores na reflexão sobre suas práticas e na elaboração do projeto educativo de sua escola. Não são regras a respeito do que devem ou não fazer. No entanto, é necessário estabelecer acordos nas escolas em relação às estratégias didáticas mais adequadas. A qualidade da intervenção do professor sobre o aluno ou grupo de alunos, os materiais didáticos, horários, espaço, organização e estrutura das classes, a seleção de conteúdos e a proposição de atividades concorrem para que o caminho seja percorrido com sucesso (BRASIL, 1997, p. 68).

Portanto, os alunos de uma maneira geral, são direcionados pelos Parâmetros Curriculares Nacionais e estes indicam como objetivos do ensino fundamental que os alunos sejam capazes de:

> Compreender a cidadania como participação social e política, assim como exercício de direitos e deveres políticos, civis e sociais, adotando, no dia-a-dia, atitudes de solidariedade, cooperação e repúdio às injustiças, respeitando o outro e exigindo para si o mesmo respeito; Posicionar-se de maneira crítica, responsável e construtiva nas diferentes situações sociais, utilizando o diálogo como forma de mediar conflitos e de tomar decisões coletivas; Conhecer características fundamentais do Brasil nas dimensões sociais, materiais e culturais como meio para construir progressivamente a noção de identidade nacional e pessoal e o sentimento de pertinência ao País; Conhecer e valorizar a pluralidade do patrimônio sociocultural brasileiro, bem como aspectos socioculturais de outros povos e nações, posicionando-se contra qualquer discriminação baseada em diferenças culturais, de classe social, de crenças, de sexo, de etnia ou outras características individuais e sociais; Perceber-se integrante, dependente e agente transformador do ambiente, identificando seus elementos e as interações entre eles, contribuindo ativamente para a melhoria do meio ambiente; Desenvolver o conhecimento ajustado de si mesmo e o sentimento de confiança em suas capacidades afetiva, física, cognitiva, ética, estética, de inter-relação pessoal e de inserção social, para agir

> com perseverança na busca de conhecimento e no exercício da cidadania; Conhecer e cuidar do próprio corpo, valorizando e adotando hábitos saudáveis como um dos aspectos básicos da qualidade de vida e agindo com responsabilidade em relação à sua saúde e à saúde coletiva; Utilizar as diferentes linguagens — verbal, matemática, gráfica, plástica e corporal como meio para produzir, expressar e comunicar suas ideias, interpretar e usufruir das produções culturais, em contextos públicos e privados, atendendo a diferentes intenções e situações de comunicação; Saber utilizar diferentes fontes de informação e recursos tecnológicos para adquirir e construir conhecimentos; Questionar a realidade formulando-se problemas e tratando de resolvê-los, utilizando para isso o pensamento lógico, a criatividade, a intuição, a capacidade de análise crítica, selecionando procedimentos e verificando sua adequação sucesso (BRASIL, 1997, p. 69).

Por fim, vale lembrar que os objetivos gerais do ensino fundamental e os objetivos gerais de área para o ensino fundamental sofreram algumas reformulações de tal modo a atender e respeitar a diversidade social e cultural de cada região.

Os Parâmetros Curriculares Nacionais do ensino fundamental tem diretrizes voltadas para a preparação dos alunos para o ensino médio, ou seja, cada aluno precisa chegar ao próximo nível de ensino com conceitos básicos a respeito de cada disciplina.

2.1 Os PCN'S de Matemática no Ensino Fundamental

A Matemática é bem ampla como ciência e como disciplina, cada modulo precisa ser muito bem abordado pelo professor para que não sejam gerados conflitos ou complicações futuras, ou seja, comporta um amplo campo de relações, regularidades e coerências e que naturalmente despertam a curiosidade e instigam a capacidade de generalizar, projetar, prever e abstrair, o que acaba gerando um favorecimento quanto à estruturação do pensamento e o aluno, principalmente, é despertado para um novo desenvolvimento do raciocínio lógico.

A matemática está presente no cotidiano das pessoas, sejam estudantes ou não, todos os dias de uma forma ou de outra fazemos cálculos ou operações sem perceber, ou seja, o ato de contar, comparar e operar sobre quantidades, tudo isso é pura matemática.

De acordo com Brasil (1997, p. 37) "Nos cálculos relativos a salários, pagamentos e consumo, na organização de atividades como agricultura e pesca, a Matemática se apresenta como um conhecimento de muita aplicabilidade". Assim, empresas utilizam a matemática com bem mais frequência.

A matemática praticamente está em todo o lugar e acaba sendo agregada a várias áreas do conhecimento, ou seja, diferentes áreas do conhecimento, principalmente porque se utilizada em estudos ligados às ciências da natureza e as às ciências sociais, além disso, consegue fazer parte de composições musicais, na coreografia, na arte e nos esportes.

De acordo com os PCN'S de matemática, as finalidades do ensino dessa disciplina indicam, como objetivos do ensino fundamental, levar o aluno a:

> Identificar os conhecimentos matemáticos como meios para compreender e transformar o mundo à sua volta e perceber o caráter de jogo intelectual, característico da Matemática, como aspecto que estimula o interesse, a curiosidade, o espírito de investigação e o desenvolvimento da capacidade para resolver problemas; Fazer observações sistemáticas de aspectos quantitativos e qualitativos do ponto de vista do conhecimento e estabelecer o maior número possível de relações entre eles, utilizando para isso o conhecimento matemático (aritmético, geométrico, métrico, algébrico, estatístico, combinatório, probabilístico); selecionar, organizar e produzir informações relevantes, para interpretá-las e avaliá-las criticamente; Resolver situações-problema, sabendo validar estratégias e resultados, desenvolvendo formas de raciocínio e processos, como dedução, indução, intuição, analogia, estimativa, e utilizando conceitos e procedimentos matemáticos, bem como instrumentos tecnológicos disponíveis; Comunicar-se matematicamente, ou seja, descrever, representar e apresentar resultados com precisão e argumentar sobre suas conjecturas, fazendo uso da linguagem oral e estabelecendo relações entre ela e diferentes representações matemáticas; Estabelecer conexões entre temas matemáticos de diferentes campos e entre esses temas e conhecimentos de outras áreas curriculares; Sentir-se seguro da própria capacidade de construir conhecimentos matemáticos, desenvolvendo a auto-estima e a perseverança na busca de soluções; Interagir com seus pares de forma cooperativa, trabalhando coletivamente na busca de soluções para problemas propostos, identificando aspectos consensuais ou não na discussão de um assunto, respeitando o modo de pensar dos colegas e aprendendo com eles (BRASIL, 1997, p. 37).

Em outras palavras as crianças que ingressam no primeiro ciclo, mesmo tendo ou não passado pela pré-escola, tem em seu conhecimento uma bagagem de noções informais sobre numeração, medida, espaço e forma, construídas em sua vivência cotidiana. Essa noção é de fundamental importância para o professor, pois a partir desse ponto ele tem uma referência mais precisa na organização das formas de aprendizagem.

2.2 Dificuldades de Aprendizagem em Matemática

No que diz respeito às dificuldades de aprendizagem em matemática, elas podem ser trabalhadas com êxito a partir de tarefas conjuntas com professores, pais, alunos e também com o apoio do sistema de ensino. O relacionamento dos alunos com as pessoas que o rodeiam pode entusiasmar bastante no desenvolvimento das atividades exigidas para eles, bem como a formação, o método de ensino e avaliação podem ajudar ou atrasar o processo de ensino e aprendizagem do indivíduo:

> A resolução de problemas, na perspectiva indicada pelos educadores matemáticos, possibilita ao aluno mobilizar conhecimentos desenvolvera capacidade para gerenciar as informações que estão a seu alcance. Assim, os alunos terão oportunidade de ampliar seus conhecimentos acerca de

> conceitos e procedimentos matemáticos bem como de ampliar a visão que têm dos problemas, da Matemática, do mundo em geral e desenvolver sua autoconfiança. (BRASIL, 1998, p.40)

Por esse motivo faz-se necessário a uso da calculadora, pois esse recurso serve como instrumento facilitador do aprendizado, desde que o aluno consiga identificar e interpretar a finalidade da máquina. A utilização errônia das tecnologias ou qualquer outro método danifica o desenvolvimento de habilidades e competências adquiridas pelos alunos.

Há métodos que podem facilitar a vida dessas pessoas quando precisam da matemática. Para aperfeiçoar o seu desempenho, o professor deve deixar que o sujeito utilize tabuada, calculadora, cadernos quadriculados e elaborar exercícios e provas com enunciados mais claros e diretos. Além disso, pode estimular o indivíduo passando trabalhos de casa com exercícios repetitivos e cumulativos.

O processo de ensino-aprendizagem tem cada vez mais preocupado alguns profissionais, independente da área educativa, pois os mesmos estão procurando soluções para sanar tais dificuldades, em se tratando de sala de aula. Felizmente algumas tentativas estão sendo feitas a respeito da importância da disciplina de matemática, buscando amenizar essa situação, bem como o lançamento de propostas ou ideias com foco principal de levar uma quantidade cada vez maior para entendimento e compreensão da matemática.

Para D'Ambrosio (1997, p. 124) "O ensino da matemática avançou nas últimas décadas aumentando o valor dos aspectos psicológicos além dos metodológicos no processo de ensino aprendizagem". Em pleno século XXI, pode-se perceber que o homem de maneira geral está rodeado de tecnologia por todas as partes, o que passa a exigir do mesmo, respostas em tempo hábil, diversas situações, problemas a serem resolvidos. Resumindo, a matemática é essencial e de fundamental importância em varias áreas de conhecimento.

Conforme o Brasil (1998), os PCN's "É importante destacar que a matemática deverá ser vista pelo aluno, como um conhecimento que pode favorecer o desenvolvimento do seu raciocínio, de sua sensibilidade expressiva, de sua sensibilidade estética e de sua imaginação". PCN's trabalham com intuito não apenas de conseguir uma simples mudança com relação a matemática, mas sim de implantar uma filosofia diferente de ensino e aprendizagem. O objetivo real é a mudança urgente dos métodos de ensino, porém não apenas em ensinar cada vez mais, ou seja, de maneira exaustiva, mas há meios específicos e melhores de como se ensinar e avaliar o aluno, para que sejam organizadas situações melhores de ensino e de aprendizagem.

Conforme a história, o processo de ensinamento da matemática ficou marcado por muitos conflitos entre professores e alunos. Ramos (1987, p. 48) "É necessário mudar essa concepção negativa, e quebrar algumas barreiras, tabus que trazemos conosco em relação à matemática e consequentemente conhecê-la, pois ninguém gosta do que não conhece".

> Qual a reação dos nossos alunos quando o assunto é Matemática? Essa inquietação me deixa cada dia mais "inconformado" em relação ao ensino da Matemática no contexto escolar, visto que a mesma faz parte da nossa vida diária e, no entanto muitos de nossos alunos se julgam incapazes de compreender essa ciência. (POLYA, 1995, p. 62).

Alguns confrontos começam a surgir no que diz respeito ao ensino da matemática, ou seja, o choque entre o novo e o velho, as diferenças identificadas, concepções e hipóteses existentes, esse contexto faz com que o aluno comece a ampliar mesmo que devagar seus conhecimentos de forma organizada. Para D'Ambrósio (1997):

> Atualmente, a Matemática vem passando por uma grande transformação. Isso é absolutamente natural. Os meios de observação, de coleção de dados e de processamento desses dados, que são essenciais na criação Matemática, mudaram profundamente. Não que se tenha relaxado o rigor, mas, sem dúvida, o rigor científico hoje é de outra natureza. (D'AMBRÓSIO, 1997, p. 42).

A disciplina de matemática pode ser atribuída a um caráter diferente, ou seja, passando a ser uma necessidade real da sociedade, com a capacidade de resolver operações básicas relacionadas a sociedade em geral.

Ramos (1987, p. 47), comenta bem quando diz que "A deficiência maior na aprendizagem matemática é a transmissão do conteúdo pouco contextualizado, segundo vem acontecendo a tempos nas escolas, dando desmotivação ao aluno".

Os professores precisam lecionar aulas mais dinâmicas, para de fato chamar a atenção do aluno, dando um motivo simples de que tanto a aula como o conteúdo ministrado são importantes não apenas para o espaço escolar, mas também fazer com que o aluno perceba a importância de aprender a matemática para ser usado além dos muros da escola.

Entretanto para Rangel (1992, p. 250), "Os alunos que aprendem sem realmente compreender o que fazem, esquecem facilmente quando deixam de fazer isso. Só se aprende quando fazem com frequência, pois não há uma tomada de consciência sobre o que fazer".

A matemática tem uma espécie de intimidade muito pessoal. Para que se possa estudar e aprender verdadeiramente a disciplina requer do aluno uma atitude muito pessoal, isso se aplica também a quem ensina não basta apenas conhecer, é preciso criar e inovar.

Um ensino voltado somente para a realização com êxito em exercícios, aplicando regras, causam uma falha na compreensão, ou seja, na construção de um conhecimento lógico matemático.

A matemática é uma ciência que não dá pra desenvolver se for decorada, tem que ser realmente aprendida, é importante raciocinar, pois com isso o aprendizado do aluno é garantido e a tendência de erro também diminui.

> É difícil imaginar um problema absolutamente novo, sem qualquer semelhança ou relação com qualquer outro que já haja sido resolvido; se tal problema pudesse existir, ele seria insolúvel. De fato, ao resolver um problema sempre aproveitamos algum problema anteriormente resolvido, usando o seu resultado, ou o seu método, ou a experiência adquirida ao resolvê-lo. (POLYA, 1995, p. 36).

Entretanto, muitos alunos, mesmo depois de concluir o ensino médio, encontram dificuldades de generalizar a matemática, ou seja, de reconhecer um objeto da disciplina, como por exemplo, números naturais, inteiros, racionais, figuras geométricas entre outros.

Rangel (1992, p. 250) diz que "O grande erro do ensino da matemática tem sido o de estar voltado para a aprendizagem superficial de regras e de toda linguagem de sinais operatórios".

A matemática parte do conceito de ser sem sombra de dúvidas a ciência que melhor permite o trabalho mental e ajuda a desenvolver e aperfeiçoar o raciocínio que se aplica a qualquer assunto.

Para Barbosa (2008, p. 15), "a aprendizagem decorre da ação do aprendiz sobre o mundo e dos elementos deste mundo que agem sobre ele, caracterizando-se uma ação dialética, modificando, portanto, a concepção do que seja ensinar".

Porém, há um público que é totalmente contrário ao pensamento do autor, pois tem dificuldades de aprendizagem, que precisam de uma atenção muito maior que os demais.

Para Fonseca (1995, p. 9), "A investigação em Dificuldades de Aprendizagem (DA) tem sido controversa e fundamentalmente pouco produtiva no que respeita a um melhor controle e compreensão das suas causas e consequências".

É importante fazer uma análise histórica sobre a problemática da aprendizagem ou das Dificuldades de Aprendizagem (DA), onde se pode fazer um paralelo com relação ao desenvolvimento da sociedade em decorrência das dificuldades de aprendizagem.

> Nos séculos XIII e XIV, a entrada para a escola se dava por volta dos 13 anos. No século XVI, os jesuítas estabeleceram a entrada para a escola aos sete anos e criaram as "classes de nível" que podiam ter crianças de oito anos e adultos de 24 anos. No século XVII, os reinados de Luís XIII e Luís XIV, a entrada para a escola é criada aos nove e aos cinco anos, respectivamente. Em pleno século XVIII, as mudanças de atitude decorrentes da filosofia de Rousseau e de Diderot levam ao "ensino para todos e na base da diversidade". Mais tarde, já no século XIX e XX, as ideias de Montessori, Decroly, Froebel, Dewey, Makarenko, Mendel, Freinet e tantos outros reforçam a necessidade da escola estar aberta à vida, ao mesmo tempo que deveria ser obrigatória para todos e não só para os filhos dos favorecidos ou privilegiados.(FONSECA, 1995, p. 9).

Em decorrência dessa simples abordagem, pode-se chegar a seguinte conclusão: a escola com o passar do tempo foi impondo exigências, mesmo assim conseguiu proporcio-

nar a abertura de um maior número de crianças na escola, aumentado também a taxa de escolarização. E quando os métodos implantados não serviam para todas as crianças, de maneira rápida, se criavam novos métodos para que as outras fossem atendidas.

A grande maioria de pais tem uma visão totalmente errada da escola, "sempre mandam as crianças para a escola para aprender", mas não funciona tão simples assim, há um processo por trás disso tudo e é preciso que os pais entendam todo ele. As crianças não podem mais continuar a ser simples vítimas de quaisquer tipos de métodos, por mais populares que sejam.

> Temos que ajustar as condições internas de aprendizagem, isto é, as condições da criança (o que pressupõe um estudo aprofundado do seu desenvolvimento biopsicossocial) às exigências das tarefas educacionais, ou seja, às condições externas da aprendizagem, ou melhor, às condições de ensino inerentes ao professor e ao sistema de ensino, ou seja, aos seus processos de transmissão cultural.(FONSECA, 1995, p. 9-10)

A aprendizagem e a construção do conhecimento são procedimentos naturais e espontâneos do ser humano que desde muito cedo aprende a mamar, falar, andar, pensar, garantindo assim, a sua sobrevivência. Aproximadamente aos três anos, as crianças são hábeis de construir as primeiras hipóteses e já começam a questionar sobre a existência.

A aprendizagem escolar também é entendida como um processo natural, resultado de uma difícil atividade mental, na qual o pensamento, a percepção, as emoções, a memória, a motricidade e os conhecimentos prévios estão envolvidos e é nesse momento que a criança deve sentir o prazer em aprender.

Segundo Selikowitz (2001, p.4), sobre a dificuldade de aprendizagem diz que "É uma condição inesperada e inexplicável, que ocorre em uma criança de inteligência media ou superior, caracterizada por um atraso significativo em uma ou mais áreas de aprendizagem". Por esse motivo, quando se fala em dificuldade de aprendizagem é importante que todos aqueles que estão ao redor do sujeito que a apresenta devam estar atentos e assim tomar as medidas necessárias para melhorar ou ate mesmo sanar essa dificuldade. Isso por meio de profissionais qualificados como o psicopedagogo e psicólogos. São eles os responsáveis no estudo do processo de aprendizagem humana e suas dificuldades, levando-se em consideração as realidades interna e externa, utilizando-se de vários campos da ciência, integrando-os e sintetizando-os. Buscando compreender de forma global e integrada os processos cognitivos, emocionais, orgânicos, familiares, sociais e pedagógicos que determinam suas condições.

As dificuldades relacionadas com a aprendizagem raramente têm origens apenas cognitivas. O âmbito escola, também pode ser considerado uma das causas que podem conduzir o aluno ao fracasso escolar. Não podemos desconsiderar que o fracasso do aluno

também pode ser entendido como um fracasso da escola por não saber lidar com a diversidade dos seus alunos.

Portanto, é preciso que o professor atente para as diferentes formas de ensinar, pois, há muitas maneiras de aprender. O professor deve ter consciência da importância de criar vínculos com os seus alunos através das atividades cotidianas, construindo e reconstruindo sempre novos vínculos mais fortes e positivos, trazendo a família para junto desse processo de aprendizagem.

Cada pessoa é única, com uma vida e uma história de vida, por isso, precisa-se saber o aluno que tem e como ele aprende. Se ele construiu algo, não se pode destruí-la. O psicopedagogo ajuda a promover mudanças, intervindo diante das dificuldades que a escola nos coloca, trabalhando com os equilíbrios/desequilíbrios e resgatando o desejo de aprender.

O que se pode afirmar é que nem todos os alunos não gostam da disciplina de matemática, a mesma ainda divide opiniões diferentes, assim diz Druck (2003, p. 21) "A matemática não é uma disciplina de total rejeição, podemos dizer que ela é "querida por muitos e odiada por outros", ou "o aluno gosta ou ele não gosta de matemática". O ideal é que a matemática seja uma disciplina mais trabalhada, ou seja, que tenha mais atenção por parte tanto dos alunos, quanto de professores para que esse quadro seja totalmente revertido.

Novas formas ou estratégias didáticas devem ser encontradas, de acordo com Orlandi (2004, p. 16) "É necessário reformular os objetivos e repensar na finalidade de avaliar e analisar os erros, ajudando o aluno a viver a matemática". Podem ser destacadas nesse momento algumas atitudes dos professores que poderiam viabilizar e ao mesmo tempo melhorar a aceitação das aulas de matemática tais como: melhoria no processo explicativo, tentando sempre explicar da forma mais clara possível e se dando conta que nem sempre todos os alunos encontram-se no mesmo nível; qualidade nas aulas, sendo as mesmas mais dinâmicas e consequentemente mais interessantes; diminuir a aceleração da matéria, ou seja, revisando os pontos mais importantes; uma atenção individual aos alunos, especialmente aos que encontram mais dificuldade.

O treinamento realizado da maneira correta em matemática é resultado de um argumento lógico mais eficiente, capacidade de distinguir casos e resolver problemas, possibilidade da critica dos resultados alcançados, provocando assim um pensamento ou raciocínio mais independente.

Os professores que lecionam matérias de exatas, que é onde os alunos encontram menos afinidade, se deparam com algumas dificuldades, porém a primeiro momento o que deve ocorrer é a quebra da distância entre aluno e professor, mostrando que o professor busca sempre ajudar e não punir. O respeito deve ocorrer de ambos os lados, pois isso

já ajuda a tirar uma barreira negativa dessa disciplina. O que se encontra em algumas instituições de ensino são professores com mentalidades antigas, que se colocam como os donos da verdade, assim a dificuldade de ensino somente aumenta.

A boa verdade na disciplina de matemática é que ela é uma matéria que proporciona uma interação diferente de outras, a troca de informações passa a ser bem divertida e emocionante, podendo ser criadas diversas estratégias que provoquem a mente dos alunos a sempre querer mais, uma espécie de disputa sadia.

2.3 Estratégias Metodológicas para Melhoria da Aprendizagem

A disciplina de matemática enfrenta muitas dificuldades e resistência, em se tratando da motivação já se torna um assunto muito complexo, ou seja, depende muito do professor depositar todo carinho, gosto, dedicação e empenho na sua atividade, com isso a possibilidade de se criar um ambiente mais agradável é maior, ambiente esse em que o aluno se mostre ansioso com o aprendizado e acabe com o medo de errar.

A participação do professor é algo fundamental, não tirando a responsabilidade do aluno que também é muito válida, mas o mestre não pode cair na mesmice e ensinar da mesma forma que outros já ensinaram. De acordo com Orlandi (2004, p. 16) "Essas concepções de aprendizagem exigem uma nova ação pedagógica que favoreça o "aprender a aprender" e o desenvolvimento de competências por meio de estratégias que mobilizam mais o raciocínio do que a memória".

É importante que o aluno durante o seu processo de ensino se torne capaz de:

> Usar a matemática como instrumento para ampliar seus conhecimentos; Utilizar os conhecimentos adquiridos em situações do dia-a-dia, como forma de interação com seu meio; Usar estruturas de pensamento que sejam suporte para conhecimento matemático; Valorizar o raciocínio abstrato e a linguagem simbólica; Ampliar a visão espacial (tempo, espaço); Explorar o raciocínio intuitivo; Compreender o papel da interação na aquisição do conhecimento; Perceber que a disciplina estimula o interesse; Resolver situações-problema adotando estratégias, bem como utilizar recursos tecnológicos disponíveis diante de alguma situação; Desenvolver a auto-estima na busca de soluções; Interagir com os colegas de forma corporativa. (SILVA, 2004, p. 15)

As ideias que são analisadas da disciplina de matemática e os objetivos que a mesma busca, podem se bem trabalhados, constituir um novo caminho, ou seja, é possível elaborar novas estratégias que venham a solucionar os problemas dessa disciplina.

É interessante que os professores de matemática e educadores de maneira geral, vejam que a matemática é uma ciência em continua evolução, que precisa de muita atenção, pois a mesma responde muitos problemas e já chegou a ser crucial na cultura do homem.

3 CRIPTOGRAFIA: HISTORICIDADE

Durante muitos anos, até os dias de hoje, inúmeros acontecimentos marcaram época e ficou gravado na história, a criptografia é um delas. Assim, nesse capítulo, alguns eventos históricos com envolvimento direto da criptografia serão explanados, assim como a evolução dos métodos de cifragem, onde são fornecidos dados importantes para que o professor de matemática possa introduzir a criptografia no ensino básico.

A criptografia surge através da necessidade de transmissão de mensagens confidenciais, onde somente o emissor e o receptor podem decifrar. Todavia, juntamente com essa necessidade há quem precise ou necessite interceptar ou decifrar mensagens, e os motivos da época eram muitos, por exemplo, segredos militares, políticos, religiosos, comércio e porque não as mensagens sentimentais.

Os estudiosos consideram como primeiro documento de escrita cifrada existente, alguns hieróglifos egípcios, estes foram encontrados na tumba de Khnumhotep, a aproximadamente 1900 a.C. Porém, ainda em 1500 a.C. aproximadamente houve o desenvolvimento da esteganografia pelas culturas egípcia, chinesa, indiana e mesopotâmica. Assim, algumas situações eram como mensagens passadas, como por exemplo, raspar o cabelo, tatuar uma mensagem, deixar o cabelo crescer, enviar ao destinatário que raspará novamente para que a leitura seja efetuada (GOMES, 2014).

O desenvolvimento da criptografia desde tempos antigos até a atualidade é marcado por três grandes fases: Artesanal, Mecânica e Digital.

A divisão é bem interessante e tem a vantagem de oferecer uma visão geral sobre todos os ângulos, porém, possui de certa forma, certa imprecisão, sendo impossível determinar exatamente quando uma fase começa e a outra termina.

Dessa forma, apresenta-se um resumo sobre a história da Criptografia, objetivando entender sua utilidade ao longo da história.

3.1 Criptografia Artesanal

O período artesanal registra os primeiros indícios de utilização da criptografia, paralelamente com o surgimento da escrita, ocorrendo durante a idade antiga e média.

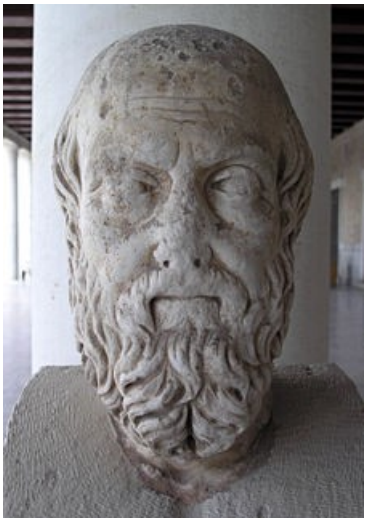
Segue uma sequencia de relatos históricos que destacam este período. Estas técnicas têm em comum o fato de poderem ser empregadas usando-se apenas lápis e papel, e poderem ser decifradas praticamente da mesma forma. Atualmente com a ajuda dos computadores, as mensagens criptografadas empregando-se estes algoritmos são facilmente

decifradas, por isso caíram rapidamente em desuso.

3.1.1 Heródoto

Heródoto pode ser considerado um dos pioneiros na área da escrita, pois uns dos primeiros textos sobre códigos secretos foi escrito por ele, geografo e historiador o grego Heródoto (485 a.C. - 420 a.C.) teve papel importante na história da criptografia. De acordo com Heródoto a Grécia foi salva da conquista por Xerxes (Rei dos Reis da Pérsia) graças a técnica da escrita secreta (SINGH, 2004).

Figura 1 – Busto de Heródoto



Fonte:https://pt.wikipedia.org/wiki/História

O historiador também faz ressalva a história de Histaeu que para transmitir suas instruções com segurança, precisou raspar a cabeça do mensageiro, escrevendo a mensagem no couro cabeludo e aguardou até que o cabelo voltasse a crescer. O mensageiro seguiu seu caminho e quando chegou ao seu destino, raspou novamente a cabeça revelando a mensagem ao destinatário (SINGH, 2004).

3.1.2 O Bastão de Licurgo

Os espartanos usavam o scytale ou como também pode ser chamado de “bastão de Licurgo”, uma cifra de transposição, para transmitir mensagens extremamente confidenciais. O bastão de Licurgo foi considerado o primeiro aparelho criptográfico utilizado pelos militares, criado no século V a.C. Era um bastão de madeira ao redor do qual se enrolava uma tira de couro longa e estreita (MALAGUTTI, 2009).

Figura 2 – Bastão de Licurgo

Fonte:https://pt.wikipedia.org/wiki/Cítala

O bastão funcionava da seguinte forma, bastava o remetente escrever a mensagem ao longo do comprimento do instrumento e logo depois somente precisava desenrolar a fita, formando uma mensagem contendo letras sem sentido (MALAGUTTI, 2009).

3.1.3 Código de César

O famoso Júlio Cesar (por volta de 60 a.C.), conhecido por muitas pessoas, usava um cifrario para comunicar suas estratégias de batalha aos generais de seu exército.

Figura 3 – Código de César

Original	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrado	d	e	f	g	h	i	j	k	l	m	n	o	p

Original	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	q	r	s	t	u	v	w	x	y	z	a	b	c

Fonte:http://www.pythondiario.com/2015/04/cifrado-cesar-en-python-caesar-cipher.html

O general Júlio Cesar tinha sua própria correspondência particular onde utilizava um código de substituição muito simples “no qual cada letra da mensagem original era substituída pela letra que a seguia em três posições no alfabeto: a letra A era substituída por D, a B por E, e assim até a última letra Z, que é cifrada com a letra C” (FRANÇA, 2014).

3.1.4 O cifrário de Francis Bacon

O Cifrário de Francis Bacon, (filósofo, escritor e político inglês), por volta do século XVI, detalhou sua forma de escrita, ou seja, através de seu sistema de substituição usando um alfabeto de 24 letras onde I = J e U = V.

Figura 4 – Cifrário de Francis Bacon

Letra	Grupo	Binário		Letra	Grupo	Binário
A	aaaaa	00000		N	abbaa	01100
B	aaaab	00001		O	abbab	01101
C	aaaba	00010		P	abbba	01110
D	aaabb	00011		Q	abbbb	01111
E	aabaa	00100		R	baaaa	10000
G	aabba	00110		T	baaba	10010
H	aabbb	00111		U/V	baabb	10011
I/J	abaaa	01000		W	babaa	10100
K	abaab	01001		X	babab	10101
L	ababa	01010		Y	babba	10110
M	ababb	01011		Z	babbb	10111

Para cada uma das letras do alfabeto é atribuído um grupo de 5 caracteres compostos pelas letras **a** e **b**. Como são utilizadas apenas duas letras para a formação dos grupos, considera-se esta cifra como binária. Como os grupos são formados por 5 letras, considera-se a cifra como sendo de 5 bits e cada caractere possui duas possibilidades, podendo assim gerar 32 grupos e consequentemente representar 32 letras distintas. A formação dos grupos segue uma sequência lógica fácil de memorizar. Além disso, os **a** e **b** podem ser substituídos por 0 e 1 (FRANÇA, 2014).

3.1.5 Criptoanalistas árabes

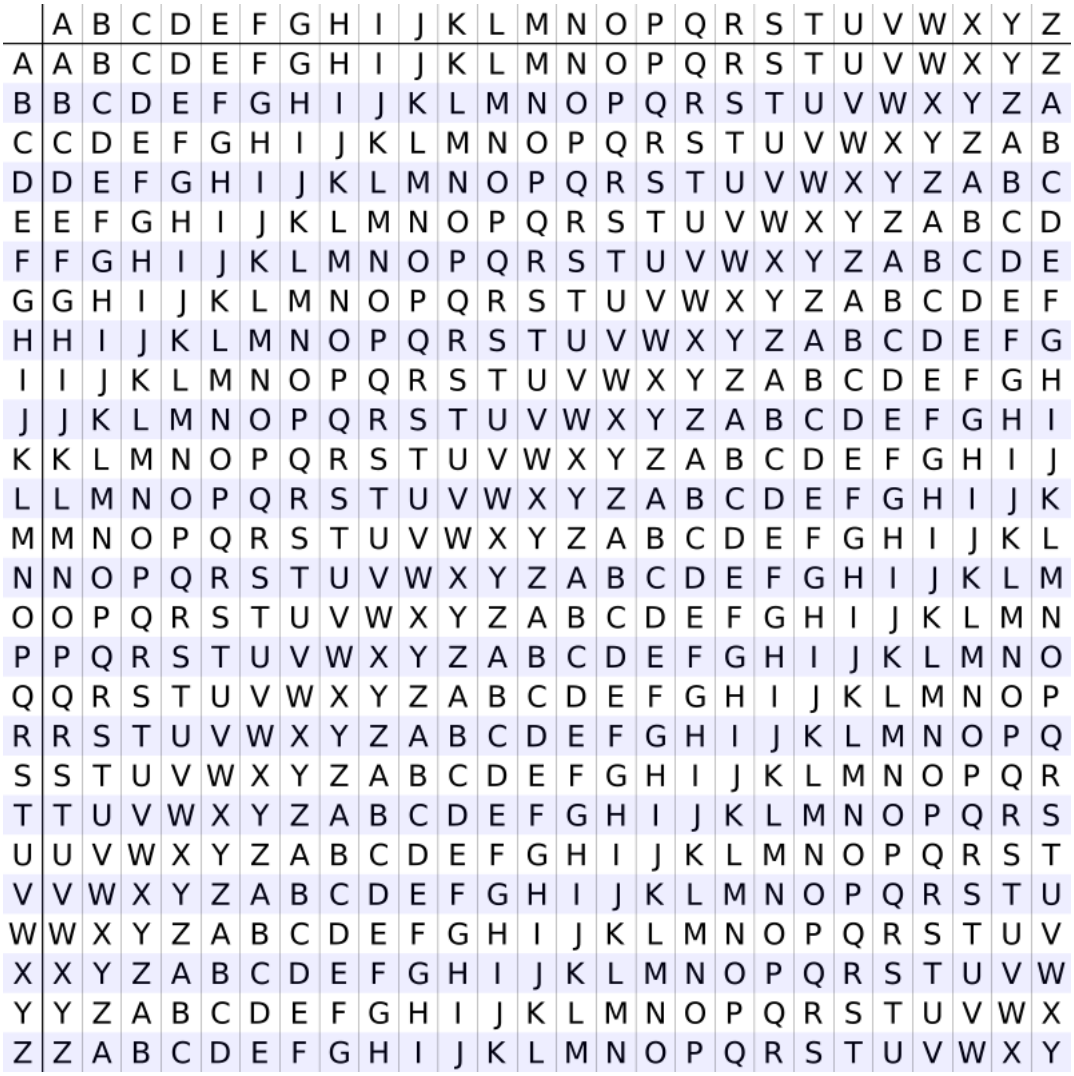
Durante muitos anos, vários estudiosos acreditavam que a cifra de forma alguma poderia ser decifrada. Porém, decifradores descobriram uma forma bem interessante de acabar com todo aquele mistério, ou seja, uma espécie de atalho para quebrar a cifra, e a mensagem acabava sendo revelado em minutos. Os responsáveis por essa descoberta localizavam-se ao Oriente Médio, eram estudiosos árabes, que utilizavam uma combinação de linguística, estatística e devoção religiosa (MALAGUTTI, 2009). “A criação da criptoanálise, a partir da definição do método da análise de frequências, deu início a uma permanente luta entre os criadores e os quebradores de códigos, o que, desde aquela época, vem beneficiando ambas as partes” (MALAGUTTI, 2009).

3.1.6 A cifra de Vigenère

Diante da fragilidade apresentada pelas cifras monoalfabéticas, isso por volta de 1640, o italiano Leon Alberti propôs uma nova modalidade de escrita, ou seja, o uso de dois ou mais alfabetos, usados alternadamente. Analisando e achando interessante essa ideia, o francês Blaise de Vigenere criou a cifra que leva seu nome. A cifra de Vigenere consiste na utilização de 26 alfabetos cifrados distintos para criar a mensagem cifrada, ou seja, para que seja decifrada uma mensagem o destinatário precisa saber que alfabeto

usar para cada letra da mensagem, e isso é previamente informado por uma palavra-chave (SINGH, 2007).

Figura 5 – Cifra de Vigenère



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

FONTE:https://pt.wikipedia.org/wiki/Cifra$_d$e$_V$igenère

Além da tabela, Vigenère também inseriu o que chamou de “palavras-chave” utilizadas tanto na codificação como na decodificação, de modo a dificultar o deciframento da mensagem criptografada.

Assim, a pessoa que codifica e a pessoa que recebe a mensagem para decodificação combinam uma palavra que será a palavra-chave do código.

Para se realizar a codificação da mensagem se repete a palavra-chave sobre as letras da mensagem a ser codificada, tantas vezes, quantas for necessário o que dependerá do tamanho da mensagem.

Como exemplo, considere que a palavra-chave seja “dado” e que se queira enviar

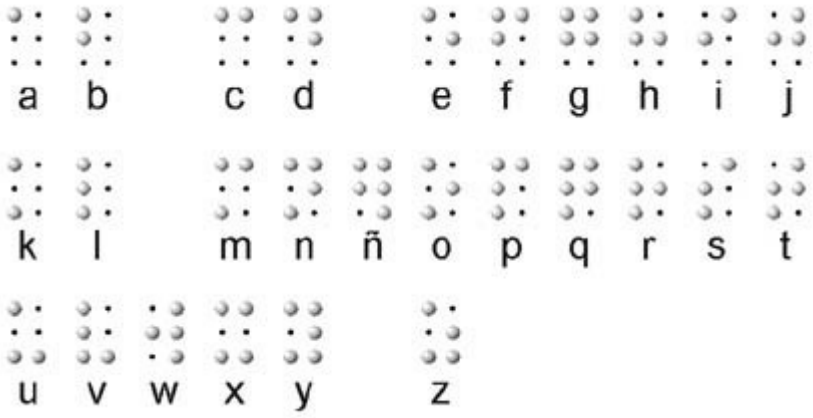
a mensagem “jogue e olhe”.

A letra da chave indica a linha que deve ser utilizada para a codificação. Deve-se considerar a linha em que o “d” está para depois analisar a coluna em que está o “j”, para, em seguida observar a intersecção entre essas duas letras, onde será encontrada a letra “m”, seguindo a regra observamos que a na linha a letra "a"e na coluna a letra "o"intersectam a letra "o". Fazendo isso com todas as letras encontramos **“mojiherzke”**

3.1.7 O código Braille

O Código Braille é hoje uma realidade, foi criado por Louis Braille (1809 - 1852), educador francês, este ficou cego logo aos 3 anos de idade. O educador acabou se interessando por um sistema de escrita, apresentado na escola Charles Barbier, no qual uma mensagem codificada em pontos era cunhada em papel cartão. Aos 15 anos de idade o educador já trabalhava numa adaptação, escrita com um instrumento simples que é um sistema de símbolos onde cada caracteres é formado por uma matriz de 6 pontos dos quais pelo menos um se destaca em relação aos outros (MALAGUTTI, 2009).

Figura 6 – Código Braille



FONTE:www.cdbraille.com

O código de braile existe em muitos países e vários dispositivos para escrita em Braille são utilizados, desde muito simples até sofisticados dispositivos eletrônicos.

3.1.8 Microponto

Em 1941, foi descoberto pelo Federal Bureau of Investigation (FBI) o primeiro microponto. Mais precisamente na Segunda Guerra Mundial, agentes alemães reduziam fotograficamente uma página de texto até que mesma chegasse ao tamanho de um ponto com menos de um milímetro de diâmetro. O receptor dessa mensagem, ao ter acesso a ela,

procurava pelo ponto com a informação e ampliava-o a fim de ler a mensagem. Durante sua descoberta, seus aliados descobriram a técnica e passaram a interceptar a comunicação (SINGH, 2004).

3.2 Criptografia Mecânica ou Quântica

A Revolução Industrial começou no final do século XVIII, na Grã-Bretanha. Ela provocou mudanças sociais, políticas, culturais e principalmente econômicas. Suas principais características foram a grande expansão e produção, que deixou de ser baseada na manufatura, e a melhoria dos transportes (SENE MOREIRA, 2000).

Diante disso, a Revolução Industrial criou no homem uma paixão muito grande pelas máquinas, ocasionando uma grande chance de substituição do já desgastante e cansativo trabalho manual pelo mecânico. No início da Idade Moderna, por exemplo, com a invenção da Imprensa, surgem os primeiros indícios da fase mecânica da criptografia.

> Neste período, iniciada na Inglaterra em 1760, seguida da invenção do telégrafo e do rádio no século seguinte, a fase mecânica se desenvolve e seu apogeu ocorre com as maquinas de cifragens usadas durante a Segunda Guerra Mundial. A máquina alemã Enigma e a mais ilustre representante desta linhagem. Na criptografia a mecânica é fundamental a ocultação pública da chave e também desejável manter segredo sobre a estrutura da maquina que produz a cifragem (FRANÇA, 2014, p. 25).

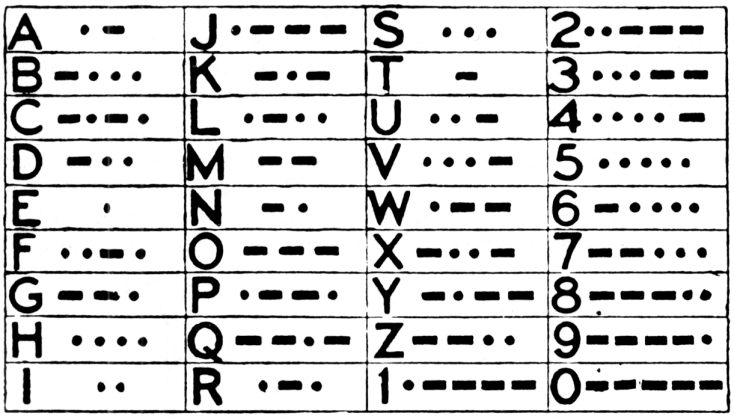
O disco de cifras, foi criado por Alberti em 1466, trata-se do primeiro sistema polialfabético conhecido, além disso, foi a primeira máquina de criptografia criada. O Disco de Cifras, conforme compreensão de França (2014, p. 26) é “um misturador que pega uma letra do texto normal e a transforma em outra letra no texto cifrado”. Mas por outro lado, o responsável pela sua invenção sugeriu que fosse mudada a disposição do disco durante uma mensagem, e isso geraria uma cifra polialfabética, proporcionando um nível maior de dificuldades a sua dedicação.

Figura 7 – Disco de cifras

FONTE:https://siriarah.wordpress.com/2014/04/23/criptografia-cifra-ou-disco-de-alberti-em-python/

O disco acelerava o trabalho e reduzia erros. Mesmo em se tratando de um dispositivo simples, foi utilizado por pelo menos uns cinco séculos.

Figura 8 – Código Morse



FONTE:http://uebto2.blogspot.com.br/p/codigo-morse-e-semaforo.html

O Código Morse foi desenvolvido em 1835, pelo pintor e inventor Samuel Finley Breese Morse, trata-se de um sistema binário de representação que funciona à distância de números, letras e sinais gráficos, absorvendo sons curtos e longos, além de pontos e traços para transmitir mensagens (FRANCISCO, 2015). Todavia, com a invenção do telefone, no fim do século XIX, o Código Morse não mais foi utilizado. Em outras palavras, mediante o desenvolvimento de tecnologias mais eficazes acabou desencadeando a substituição desse

sistema por outros aparelhos. Na França, por exemplo, o Código Morse deixou de ser utilizado pelas grandes navegações desde 1997 (FRANCISCO, 2015).

3.3 Criptografia Digital

A era que se vive hoje é da tecnologia "inúmeras são as consequências das novas tecnologias que com seu poder de multiplicador tem se voltado a quase todos os campos da esfera humana" (GRISPUN, 2009, p. 71). A tecnologia é sempre um ponto muito comentado, pois segue com o desenvolvimento e aperfeiçoamento esperado, além das máquinas terem a incrível capacidade de realizar mais de um milhão de operações por segundo. Com isso, a necessidade de uso da criptografia utilizada pelo comércio e bancos, os algoritmos criptográficos já não são reservados e passam a ser de conhecimento público, somente o segredo é que ainda está exclusivamente na chave. "Os sistemas de criptografia clássicos perderam sua eficácia devido à facilidade com que atualmente são decodificados empregando-se qualquer computador doméstico" (FRANÇA, 2014, p. 26). Portanto, quando se utilizada de um moderno computador, a informação é representada através de uma sequência de zeros e uns: são os dígitos binários, comumente conhecidos por bits. Um exemplo é o American Standard Code for Information Interchange (ASCII), (conforme figura abaixo) que destina a cada letra do alfabeto um número binário de sete dígitos, ilustrando uma sequência de zeros e uns.

Figura 9 – ASCII

Binary	Character	Binary	Character	Binary	Character
100 0001	A	110 0001	a	011 0000	0
100 0010	B	110 0010	b	011 0001	1
100 0011	C	110 0011	c	011 0010	2
100 0100	D	110 0100	d	011 0011	3
100 0101	E	110 0101	e	011 0100	4
100 0110	F	110 0110	f	011 0101	5
100 0111	G	110 0111	g	011 0110	6
100 1000	H	110 1000	h	011 0111	7
100 1001	I	110 1001	i	011 1000	8
100 1010	J	110 1010	j	011 1001	9
100 1011	K	110 1011	k		
100 1100	L	110 1100	l		
100 1101	M	110 1101	m		
100 1110	N	110 1110	n		
100 1111	O	110 1111	o		
101 0000	P	111 0000	p		
101 0001	Q	111 0001	q		
101 0010	R	111 0010	r		
101 0011	S	111 0011	s		
101 0100	T	111 0100	t		
101 0101	U	111 0101	u		
101 0110	V	111 0110	v		
101 0111	W	111 0111	w		
101 1000	X	111 1000	x		
101 1001	Y	111 1001	y		
101 1010	Z	111 1010	z		

FONTE:http://drstienecker.com/tech-261-material/29-communication-systems/

Dessa forma, durante toda esta etapa, que cobriu a fase mecânica até o princípio da fase digital com o algoritmo DES, um aspecto não sofreu qualquer alteração: a utilização de chaves privadas, caracterizando uma criptografia simétrica (veremos logo a seguir).

3.4 Criptografia Simétrica

A Criptografia simétrica trata simplesmente de um algoritmo (“programa”) que faz uma espécie de embaralhamento das informações deixando-as totalmente ilegíveis. Assim, para que a informação alcance o formato legível é necessário inserir a senha de sessão ou key session, e esta é criada no processo de encriptação.

> Na criptografia simétrica devemos escolher um algoritmo criptográfico e definir uma senha, está senha por sua vez será utilizada tanto para codificar quanto para descodificar a informação. Se você pretende enviar para alguém um arquivo codificado utilizando criptografia simétrica, seu receptor deve saber qual algoritmo foi utilizado e ter conhecimento da senha definida por você (FERREIRA, 2012 on-line).

É importante relatar que os algoritmos simétricos são bem mais rápidos do que os algoritmos assimétricos, essa diferença muita das vezes proporciona aos usuários a utilizarem a primeira opção, porém, ainda se pode usar um algoritmo assimétrico para transferir pelo menos a senha criada para o algoritmo simétrico, principalmente porque não se trata de uma informação muito extensa.

3.5 Principais Conceitos Acerca da Criptografia

Parece que sempre houve uma preocupação constante em esconder ou embaralhar as mensagens e até hoje isso vem sendo praticado, ou seja, em épocas anteriores a essa povos antigos como os egípcios, babilônios, assírios e romanos já faziam isso. Assim, quando se trata em esconder a mensagem, pode-se pensar na esteganografia. A arte da esteganografia consiste em ocultar a existência de uma mensagem (COUTO, 2008). Todavia, se houver uma intenção em impedir a leitura da mensagem por pessoas que não autorizadas para tal, modificando seus caracteres por substituição ou permutação, é utilizada a criptografia.

> A codificação é a mudança das características de um sinal com uma finalidade específica. Essa finalidade pode ser transmissão, exibição ou arquivamento. Por exemplo, pode-se converter texto, som ou imagem de forma a arquivá-los em HDs, que são dispositivos de armazenamento de dados dos computadores. Já a cifragem é alteração de símbolos(grafemas) da mensagem original como meio de torná-la acessível apenas aos autorizados (COUTO, 2008, p. 19). Entende-se por algoritmo o conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas (HOUAISS, 2009, p. 53).

Portanto, a mensagem cifrada é o resultado final da aplicação de um algoritmo invariável associado a uma determinada chave (variável ou não). Assim, tanto o sistema quanto a chave precisam ser de conhecimento do emissor e do receptor para que de fato o processo seja seguro (COUTO, 2008).

Conforme afirma Couto (2008) a criptografia convencional é composta por 5 elementos que são: o texto plano, também chamado de texto limpo ou texto claro (conteúdo original); o algoritmo criptográfico; a chave secreta; o texto cifrado e o algoritmo de decriptografia. O algo ritmo criptográfico tem a função de converter o texto limpo em texto cifrado, o algoritmo de decriptografia converte o texto cifrado em texto claro e a chave entra como um modo particular de se executar tais algoritmos.

Para tanto, o objetivo da Criptografia consiste em proteger o conteúdo de uma mensagem da curiosidade ou de malicias que seriam de interesse de pessoas não autorizadas. Como bem se sabe, a informação e uma matéria prima e ao mesmo tempo um

produto muito caro e hoje é utilizado como estratégia, diferencial competitivo (FRANÇA, 2014).

A informação é um conjunto organizado de dados, que constitui uma mensagem sobre um determinado fenómeno ou evento. A informação permite resolver problemas e tomar decisões, tendo em conta que o seu uso racional é a base do conhecimento.

> Na linguagem da criptografa, os códigos são denominados cifras, as mensagens não codificadas são textos comuns e as mensagens codificadas são textos cifrados ou criptogramas. De onde surgem duas definições: Cifrar é o ato de transformar dados em alguma forma ilegível. Seu propósito é o de garantira privacidade, mantendo a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados; e decifrar é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível (FRANÇA, 2014, p. 28).

De maneira até natural, a busca por segredos de estado, informações privilegiadas, mensagens inimigas, principalmente durante as guerras ou mais recentemente segredos industriais, além do que o ser humano também se satisfaz se auto desafiando segue estimulando a busca de métodos de quebra de cifras por meio da detecção da chave para acesso não autorizado à mensagem. Por isso, hoje em dias diversas empresas estão contratando os criptoanalistas para pesquisarem fraquezas e/ou fragilidades em sistemas por elas desenvolvidos conforme Houaiss (2009).

4 A IMPORTÂNCIA DO TEMA CRIPTOGRAFIA NO CURRÍCULO DE MATEMÁTICA DO ENSINO FUNDAMENTAL

O Ministério da Educação, principalmente na Educação Básica espera confiantemente que o estudante já esteja preparado para atuar na sociedade, a qual se faz presente, mas de forma mais efetiva, participativa, crítica, sabendo se comunicar sem dificuldades, saiba contribuir e resolver problemas do dia-a-dia e do trabalho, tomar decisões, trabalhar com eficiência e em cooperação com as demais pessoas.

Diante disso, pode ser encontrada nas Orientações Curriculares para o Ensino Fundamental(2006, p. 8), que o aluno seja capaz de utilizar a Matemática para determinadas situações, entre elas: Na resolução de problemas do cotidiano; para modelar fenômenos das distintas aéreas do conhecimento; Que a matemática se utiliza de teoremas e demonstrações; Compreender a matemática como conhecimento social e construído ao longo da história; Entender a importância da matemática no desenvolvimento científico e tecnológico.

Nesse sentido, para poder alcançar todas as finalidades e objetivos oriundos do ensino é importante um currículo que atenda aos princípios estipulados, ajudando o aluno em sua totalidade.

> Currículo é o projeto que preside as atividades educativas escolares, define suas intenções e proporciona guias de ação adequadas e úteis para os professores, que são diretamente responsáveis pela sua execução. Para isso, o currículo proporciona informações concretas sobre que ensinar, quando ensinar, como ensinar e que, como e quando avaliar.(COLL, 1999, p. 45)

Ainda, continuando no conceito do autor, o currículo é a realização do planejamento curricular, trata ainda da tomada de decisão dos objetivos que se deseja alcançar, organização dos conteúdos, elaboração das estratégias didáticas para sala de aula, definição de metodologias de ensino eficientes. Portanto, Currículo é “a estratégia para a ação educativa” (D’AMBROSIO, 1997, p. 68).

Além disso, outro ponto essencial para que seja concretizada a realização de uma aprendizagem significativa é a funcionalidade, onde:

> A educação escolar deve sempre ocupar-se de que os conhecimentos adquiridos – conceitos, habilidades, valores, normas etc – sejam funcionais, isto é, possam ser efetivamente utilizados quando as circunstâncias nas quais o aluno se encontrar assim exigirem (COLL, 1999, p. 55).

O currículo, em sua particularidade, precisa sempre levar em consideração os aspectos de funcionalidade dos conteúdos voltados para os alunos, onde se proponha atividades didáticas mais aproximadas da realidade, transportando os alunos a visualizarem a aplicabilidade dos mesmos, seja em situações dentro ou fora do ambiente escolar, no cotidiano ou na história.

A escolha de temas para o Ensino Fundamental deve ser muito bem elaborada e planejada, pois deve permitir e dar condições para que o aluno aprofunde e exercite os conteúdos já trabalhados em séries anteriores, sejam motivados a criar estratégias de resolução de problemas, tenham autonomia na resolução das atividades didáticas e trabalhem em equipe, somente assim conseguirão aprimorar a sua formação acadêmica e social.

Nesse sentido, esse ponto vai exatamente de encontro com o que é proposto no Plano Nacional de Educação (2001) que coloca que o Ensino Fundamental já deve ser uma preparação para que os estudantes enfrentem os desafios da vida moderna.

Observa-se o contexto da interdisciplinaridade, como assim é chamada, pois busca promover o crescimento das concepções de ensino, de escola, de Educação e a partir de então alterar as relações entre os segmentos que envolvem a educação: professor, aluno e conhecimento. Diante disso, na interação aluno-professor se faz necessário ambos tenham abertura para o diálogo, para as diferenças, para as experiências que cada um vive e que é relevante.

> "A interdisciplinaridade se apresenta como uma metodologia em que se respeita a especificidade de cada área, procurando estabelecer e compreender as relações entre os conhecimentos sistematizados, ampliando o espaço de diálogo na direção da negociação de ideias e da aceitação de outras visões."(PONTUSCHKA, 1993, p. 42).

Entretanto, é preciso compreender que um estudo do cotidiano não se trata somente de ficar no campo da exemplificação de fatores decorrentes do dia a dia das pessoas, está, além disso, ou seja, é usar o cotidiano como uma forma eficiente de motivação para os alunos a aprenderem conteúdos científicos.

Por fim, entende-se que trabalhar com atividades didáticas e que tem como tema principal a Criptografia prima com a possibilidade de trabalhar o desenvolvimento de atividades didáticas que proporcionem o desenvolvimento de atividades que aliam os conteúdos matemáticos a um tema que esteja ligado a atualidade, utilizando a calculadora, por exemplo.

4.1 Criptografia em Sala de Aula

O trabalho que é desenvolvido pelos profissionais da área de matemática segue sendo de extrema importância, pois conforme indica Machado (1997, p. 64) "na raiz dos processos de elaboração do conhecimento não deve escapar-lhe a captação de razões pragmáticas quase subjacentes e quase nunca suficientemente explicitadas." Além disso, é mister dizer que os matemáticos, devido às características oriundas de sua profissão, apresentam facilidade em elaborar estratégias e metodologias com a Criptografia.

A criptografia é um assunto importante e que tem despertado o interessante no contexto atual, sendo utilizado bastante em sala de aula, assim, acredita-se que seu uso possa despertar um algo a mais nos alunos, motivando-os e ajudando o professor a contornar dificuldades ao tentar estimular seus alunos, no aprendizado e conceitos relacionados com o ensino da Matemática (MACHADO, 1997).

A criptografia para ser aplicada em sala de aula precisa acompanhar um passo a passo importante, para que os alunos não se confundam com seu principal objetivo. Assim, na sala de aula, primeiramente o professor pode realizar uma aula expositiva sobre o tema, a relação da criptografia com a matemática e suas aplicações decorrentes do dia-a-dia e que muitos não percebem sua atuação. Em seguida, precisa ser apresentada a importância da comunicação para a sociedade e sua constante necessidade, surgida com o tempo, de uma linguagem secreta que permitisse sigilo entre as comunicações, abordando assim o conceito de criptografia (MACHADO, 1997).

Diante disso, chega-se a um ponto que é necessário partir para a aula prática, ou seja, uma proposta para que os alunos possam criar uma tabela com a qual fariam uma correspondência entre as letras do alfabeto e os números naturais objetivando criar um alfabeto cifrado para ser utilizado na confecção das mensagens.

4.2 Atividades Que Podem Ser Aplicadas em Sala de Aula

As aulas experimentais despertam uma curiosidade enorme nos alunos, pois através da mesma consegue-se manifestar um sentimento de curiosidade e consequentemente de vontade de aprender e fazer igual ao demonstrado pelo professor e assim obter uma aula atraente e com debate sobre as experiências realizadas (FERREIRA, 1999). Não diferente disso, as aulas relacionadas ao tema criptografia tem esse mesmo poder, pois acabam estimulando a curiosidade e acabam levando a um processo que permite a construção de novos conhecimentos.

Dessa forma, a intenção de aplicar as atividades recém elaboradas é de repassar o conhecimento obtido sobre criptografia no ambiente escolar, ou seja, na sala de aula, com orientações do professor de matemática. Assim, o tema Criptografia pode ser utilizado

como gerador eficiente de atividades didáticas que conseguem revisar, exercitar, fixar e aprofundar os conteúdos matemáticos desenvolvidos no Ensino Fundamental e Médio (OLIVEIRA, 2015).

Portanto, acredita Oliveira (2015) que com as atividades de criptografia no ensino fundamental o aluno irá usar a matemática para desvendar mensagens criptografadas. Ressalta-se ainda que nesta atividade o aluno não precisa de conhecimentos prévios. Assim, Oliveira (2015) explora o seguinte exemplo:

Codificando mensagens

Importância

Levar o aluno a codificar mensagens e/ou decodificar ou então decifrar mensagens. Professor observe que a decodificação é diferente da decifração. Quando alguém decifra uma mensagem ela quebra o código desta. Ao decodificar o código é previamente conhecido.

4.2.1 Atividade 1

Inicialmente devemos supor que a mensagem original é formada por apenas letras e espaços entre as palavras, isto é, não há nenhum número e nenhum símbolo na mensagem. Em seguida deve-se converter a mensagem numa sequência numérica

Podemos usar a conversão sugerida por COUTINHO (2003, pg. 181): A = 10; B = 11; C = 12; e assim sucessivamente até chegarmos em Y = 34 e Z = 35

Quando estiver ocorrendo à conversão das letras para os números, devemos também converter os espaços entre as palavras, que será representado por 99.

Vale lembrar ainda que as letras acentuadas ou não serão transformadas em um único número. Por exemplo, as letras A, Á, À, Ã, Â serão convertidas no número 10. Note que, se fizéssemos A corresponder ao número 1, B ao 2, C ao 3, D ao 4 e assim por diante, quando aparecesse o número 23 teríamos, desta forma, duas escolhas possíveis: BC ou W que é a vigésima terceira letra do alfabeto. Porém, ao fazer cada letra corresponder a um número com dois dígitos evitará ambiguidades.

Converta a frase **"A matemática é fascinante"** usando a sugestão anterior.

Após a conversão encontraremos a seguinte sequência numérica

10992210291422102918121099149915102812182310232914

Avaliação

Professor deve pedir para seus alunos inventarem novas frases criptografadas e distribuir para que outro colega desvende a mensagem.

4.2.2 Atividade 2

Há muito tempo povos antigos precisavam codificar mensagens para manter o devido sigilo. Seja na época antigo com Júlio Cesar, seja atualmente para fazer transações financeiras pela internet.

Converta a frase **"O professor de matemática é o mais divertido da escola"** usando o método de César.

Após a conversão encontraremos a seguinte mensagem

R SURIHVVRU GH PDWHPDWLFD H R PDLV GLYHUWLGR GD HVFROD

Avaliação

Os alunos podem criar novas frases criptografadas e distribuir para que outro aluno desvende a mensagem. Um nível mais difícil de ser decifrado seria os alunos escolherem quantas casas avançar ao invés de apenas três casas.

4.2.3 Atividade 3

Agora vamos usar o método de Vigenère para codificar uma frase.

A palavra-chave será “soma” e que se queira enviar a mensagem “A matemática é bela”.

Figura 10 – Exemplo do uso da Cifra de Vigenère.

Chave	S	O	M	A	S	O	M	A	S	O	M	A	S	O	M	A
Texto plano	A	M	A	T	E	M	A	T	I	C	A	E	B	E	L	A
Texto cifrado	S	A	M	T	W	A	M	T	A	Q	M	E	T	S	X	A

FONTE:Autor

A mensagem cifrada ficaria **SAMTWAMTAQMETSXA**

Para decodificar a mensagem basta fazer o caminho inverso desde que saiba a palavra-chave.

Figura 11 – Exemplo do uso da Cifra de Vigenère.

Chave	S	O	M	A	S	O	M	A	S	O	M	A	S	O	M	A
Texto cifrado	S	A	M	T	W	A	M	T	A	Q	M	E	T	S	X	A
Texto plano	A	M	A	T	E	M	A	T	I	C	A	E	B	E	L	A

FONTE:Autor

4.3 Criptografia RSA

O passo decisivo para a implementação do primeiro sistema criptográfico com chaves assimétricas, idealizado por Driffie, deu-se no Laboratório de Ciencia da Informação do Massachusetts Institute of Technology (MIT), por Ronald Rivest, Adi Shamir e Leonard Adleman, em 1978.

Baseia no princípio da relativa facilidade em encontrar números primos grandes e ao mesmo tempo na enorme dificuldade pratica em fatorar o produto de dois desses números, além do uso de propriedades relativamente elementares da Teoria dos Números, como a variante do Teorema de Euler.

Parte-se da procura de um sistema criptográfico com duas chaves, uma pública e outra privada, para que qualquer pessoa possa cifrar uma mensagem previamente codificada em ASCII e somente o seu legitimo destinatário possa decifra-la.

A fragilidade da mensagem através desse sistema é que se apenas cifrar cada número correspondente a um símbolo na codificação ASCII, a quebra do sistema seria imediata, pois qualquer pessoa poderia calcular tendo apenas a tabela do código ACSII, e com a correspondência (em geral não biunívoca) poderia, com uma análise de frequência na mensagem cifrada descobrir os códigos da chave a partir de sua imagem correspondente.

Essa fragilidade é resolvida traduzindo a mensagem para o código ASCII, escrevendo a mensagem traduzida de modo corrido, utilizando a sequência 0100000 para representar o espaço entre as palavras. Obtém-se assim uma longa sequência de 0 e 1. E então após uma sequência de cálculos separa-se o texto em sequencias de sete dígitos e os reconverte de ASCII para caracteres comuns e eis que aparece a mensagem.

Parece simples, mas para pôr em funcionamento precisa-se fazer muitas contas e isso só é possível com o uso de um computador. É também necessário ter acesso a números primos muito grandes e escolher com certo critério as chaves do sistema.

4.3.1 Criptografando Manualmente

Para demostrar o funcionamento do sistema RSA vamos utilizar números primos pequenos de forma que seja possível acompanhar todo o processo.

$p = 17$

$q = 11$

A seguir são calculados dois novos números n e Φ de acordo com os números p e q escolhidos:

$n = pq = 17 * 11 = 187$

$\phi = (p-1)(q-1) = 16 * 10 = 160$

Agora define-se um número e que tenha a propriedade de ser primo em relação à Φ.

Utilizaremos $e = 7$

De posse desses números começa o processo de criação das chaves públicas e privadas. É necessário encontrar um número d que satisfaça a seguinte propriedade:

$ed \equiv 1(\mod \phi)$

$d = 23$

Com esse processo definem-se as chaves de encriptação e desencriptação.

Para encriptar: utilizar e e n - esse par de números será utilizado como chave pública.

Para desencriptar: utilizar d e n - esse par de números utilizado como chave privada.

Vamos encaminhar uma mensagem bem curta de forma criptografada, como o número 4 por exemplo, tendo por base as chaves aqui estabelecidas.

Para criptografar:

- Texto original = 4

- Texto criptografado = $4^7 \equiv ($ mod 187)
- Texto criptografado = $4^7 \equiv 115($ mod 187)
- Texto criptografado = 115

Onde 115 é o resto da divisão de $4^7 por 187$

Para desencriptar:

- Texto recebido = 115
- Texto original = $115^{23} \equiv ($ mod 187)
- Texto original = $115^{23} \equiv 4($ mod 187)
- Texto original = 4

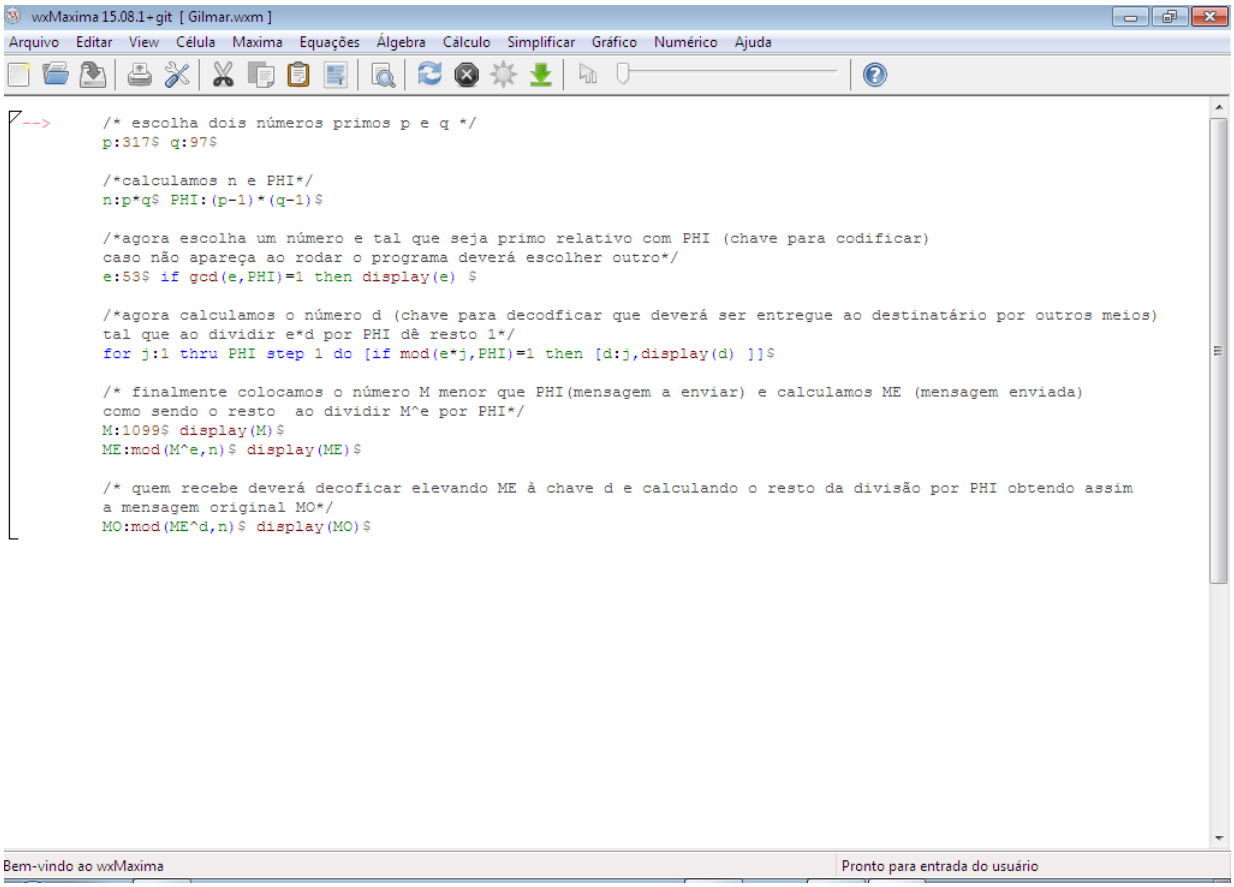
Onde 4 é o resto da divisão de $115^{23} por 187$

4.3.2 Usando o Software WxMáxima em Sala de Aula

Baixar o programa WxMáxima e instalar do site: http://maxima.sourceforge.net/download.html

Após instalar inicie o programa e abra e cole o código fonte.

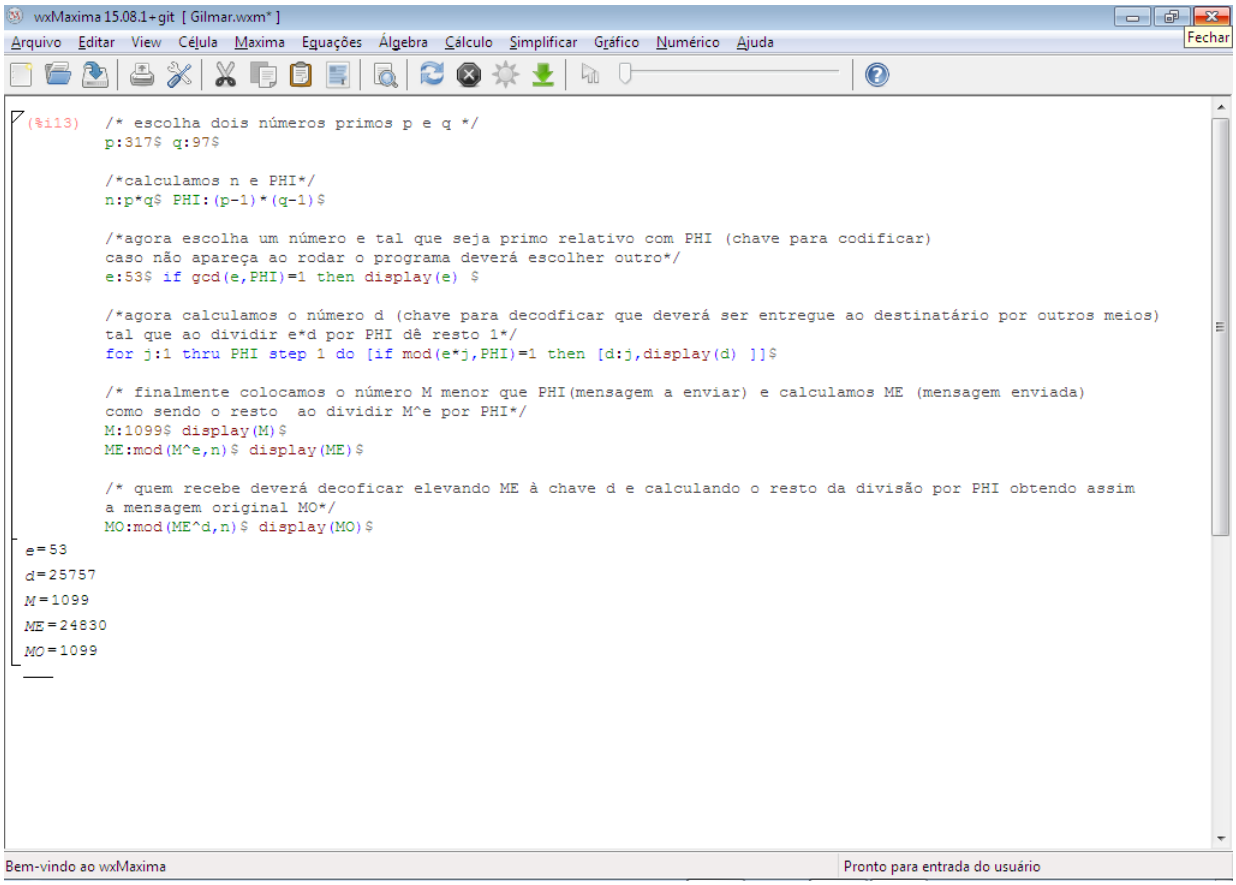
Figura 12 – Código fonte no WxMáxima



FONTE:Autor

Logo clicar em Ctrl + R para compilar o programa encontramos o seguinte resultado.

Figura 13 – Compilando no WxMáxima



FONTE:Autor

Observe que podemos mudar os números primos, a chave de codificação **e** e a mensagem a ser enviada. A chave de decodificação **d** será calculada e mostrada aumaticamente pelo programa.

5 CONSIDERAÇÕES FINAIS

O sistema educativo no Brasil passa por um momento interessante, onde mesmo que ainda poucos, mas alguns profissionais estão em busca de aperfeiçoamento profissional e qualidade de ensino, o que é de extrema importância para a melhoria do processo ensino-aprendizagem. De forma direta afeta o desenvolvimento do país, beneficiando a sociedade e as crianças que a constituem, preparando-as para enfrentar mais conscientemente as barreiras encontradas, aproveitando as oportunidades que surgirem.

É importante ressaltar que a educação é um processo continuado, que proporciona a interação das pessoas numa mesma sociedade, através de conhecimentos adquiridos pelo educando, o que resulta num padrão de comportamento adotado pelo próprio sistema escolar, devendo ser aceitos pela comunidade em que se encontram. É normal afirmar que a educação é também um processo gradativo, é adquirido por etapas, desenvolvendo o aluno mental, físico e moralmente.

Por outro lado, o sistema escolar de maneira geral, também atravessa um momento muito delicado, onde é preciso ter extrema cautela para que não sejam tomadas decisões que comprometam nem aluno, professor ou escola. Trata-se do desinteresse dos alunos pelas aulas de matemática. Todavia, acredita-se com base em renomados autores que a disciplina teórica e prática da matemática funciona perfeitamente se bem trabalhadas, especialmente quando tratamos da criptografia em sala de aula.

O estudo em questão procurou descrever os benefícios da aplicação da criptografia no ensino fundamental para melhoria do aprendizado. Assim, a criptografia é um assunto que abrange conteúdos que estão na atualidade, principalmente porque é muito utilizado no processo de comunicação, todavia este assunto não é tão aproveitado como poderia pelos discentes do Ensino Fundamental, por isso, abordou-se um tema relacionado a criptografia e seus benefícios quando aplicados em sala de aula. Segundo Groenwald e Franke (2008, p. 72), “o tema Criptografia permite interligar os conteúdos matemáticos às situações do mundo real e ajuda a desenvolver habilidades e competências na resolução de problemas”.

Sendo professor do ensino fundamental, pude levar essa ideia para dentro da sala de aula e o resultado foi muito positivo, levando em consideração que a matéria proposta aos alunos despertou curiosidade, dando a eles oportunidade de enxergar a matemática não como algo complexo e de difícil compreensão, mas sim como uma maneira de aprimorar e desenvolver o raciocínio através da criptografia. Houve interação entre eles, gerando interesse em aprender aquela forma de matemática e linguagem, alcançando assim o objetivo da educação, que é a socialização e principalmente o aprendizado.

O código fonte do RSA no WxMáxima permite modificar os dados para valores distintos garantindo o seu funcionamento. Para mensagens compridas poderiamos dividi-lá em blocos que sejam suportados pelo programa.

Portanto, os professores precisam lecionar aulas mais dinâmicas, para de fato chamar a atenção do aluno, dando um motivo simples de que tanto a aula como o conteúdo ministrado são importantes não apenas para o espaço escola, mas também fazer com que o aluno perceba a importância de aprender a matemática para ser usado para além dos muros da escola.

Referências Bibliográficas

BARBOSA, Laura Monte Serrat. Psicopedagogia: um diálogo entre a psicopedagogia e a educação. 2ª Ed. Curitiba: Bolsa Nacional do Livro, 2008.

BRASIL. Lei de diretrizes e bases da educação nacional. Conselho de Reitores das Universidades Brasileiras, 1997.

BRASIL. MINISTÉRIO DA EDUCAÇÃO. Parâmetros Curriculares Nacionais: Matemática – Ensino Médio. Brasília: Secretaria de Educação Fundamental, 1998.

BRASIL. Secretaria de Educação Fundamental. Parâmetros curriculares nacionais: introdução aos parâmetros curriculares nacionais / Secretaria de Educação Fundamental. – Brasília : MEC/SEF, 1997.

D'AMBROSIO, U. Educação Matemática da teoria a prática. 2ª Ed. Campinas: Papirus, 1997.

COSTA, Celso. Introdução à criptografia. v. 1 / Celso Costa. – Rio de Janeiro: UFF / CEP – EB, 2010.

COUTINHO, S. C. Números inteiros e criptografia. IMPA-SBM. Rio de Janeiro, 1997.

DRUCK, Suely. Artigo: O drama do ensino da matemática. Disponível em: <www1.folha.uol. com.br/folha/sinapse/ult1063u343.shtml> Acesso em 12 de Set 2015.

FONSECA, Vitor da. Introdução às dificuldades de aprendizagem. 2ª Ed. Porto Alegre: Artes Médicas, 1995.

FRANCISCO, Wagner De Cerqueria E. "Código Morse"; Brasil Escola. Disponível em <http://www.brasilescola.com/geografia/codigo-morse.htm>. Acesso em 13 de setembro de 2015.

FERREIRA, Fábio Jânio Lima. Criptografia simétrica e assimétrica. Disponível em: http://segurancadigital.info/atualizacoes-do-site/462-criptografia-simetrica-e-assimetrica. Acesso em: 12/08/2015.

FERREIRA, M. S. Investigando os rumos da disciplina escolar ciências no Colégio Pedro II: 1960-1970. Educação em Revista, Belo Horizonte, n. 45, p. 127-144, 1999.

GOMES, Francisco Claudio Lima. Uma proposta de abordagem no Ensino Médio da Criptografia RSA e sua estrutura matemática. Dissertação apresentada ao programa de Mestrado Profissional em Matemática em Rede Nacional, 2014.

GRISPUN, Mirian P. S. Zippin. Educação tecnológica: Desafios e Perspectivas. 2 ed. São Paulo: Cortez 2009.

HEFEZ, Abramo. Aritmética. 1a edição. Rio de janeiro: Sociedade brasileira de matemática. 2013.

MACHADO, Nilson José. Matemática e realidade. 4.d. São Paulo, Brasil: Cortez, 1997.

MALAGUTTI, Pedro Luiz. Atividades de Contagem a partir da Criptografia. OBMEP, Rio de Janeiro, 2009.

ORLANDI, J. C. Métodos e formas de avaliação do ensino da matemática. 2004. Monografia (Graduação em matemática). INESP/UEMG – FUNEDI, Divinópolis.

OLIVEIRA, Thais de. Criptografia. Disponível em: http://portaldoprofessor.mec.gov.br/fichaTecnicaAula.html?aula=16208. Acesso em: 13/09/2015.

OLIVEIRA, Marta Kohl de. Vygostsky aprendizado e desenvolvimento: um processo sócio histórico. São Paulo: Scipione, 2005.
PAROLIN, Isabel; HIERRO, Cristina. As dificuldades na aprendizagem e as relações familiares. Temas em Educação, v. 1, 2003.

PAROLIN, Isabel Cristina Hierro. Pais e Educadores: quem tem tempo de educar. Porto Alegre: Mediação, 2007.

PARO, Vitor Henrique. Gestão democrática da escola pública. São Paulo: Ática, 1997.

POLYA, G. A Arte de Resolver Problemas: Um novo aspecto do método matemático. Rio de Janeiro: Interciência, 1995.

PONTUSCHKA, N. (Org.). Ousadia do diálogo. São Paulo: Loyola, 1993.

RANGEL, A. C. S. Educação matemática e a construção do número pela criança. Porto Alegre: Artes Médicas, 1992.

RAMOS, L. F. O que fazer primeiro? Rio de Janeiro: Ática, 1987.

RODRIGUES, Diego de Sousa. Matriz e Criptografia: há alguma relação? Disponível em: http://portaldoprofessor.mec.gov.br/fichaTecnicaAula.html?aula=45417. Acesso em: 15/07/2015.

SELIKOWITZ, Mark. Dislexia e outras dificuldades de aprendizagem. Rio de Janeiro: Revinter Ltda. 2001.

SENE, Eustaquio de; MOREIRA, João Carlos. Espaço Geográfico mundial e globalização. São Paulo: Scipione, 2000.

SILVA, I. T da. Instrumentação para o ensino da matemática. Lavras: Unilavras, 2004. Apostila.

SINGH, Simon. O livro dos códigos. Editora Record, 2004.

SZYMANSKI, Heloisa. A relação família/escola. 2.ed. São Paulo: Liber editora, 2009.