ANA PAULA FERREIRA DOS SANTOS

A CRIPTOGRAFIA NO ENSINO FUNDAMENTAL II: CONTEXTO HISTÓRICO, CIFRAS SIMÉTRICAS, APLICAÇÕES DE CONTEÚDOS MATEMÁTICOS E MUITAS OUTRAS CURIOSIDADES.

UNIVERSIDADE ESTADUAL DO NORTE FLUMINENSE
DARCY RIBEIRO - UENF
CAMPOS DOS GOYTACAZES - RJ

OUTUBRO DE 2016

ANA PAULA FERREIRA DOS SANTOS

A CRIPTOGRAFIA NO ENSINO FUNDAMENTAL II: CONTEXTO HISTÓRICO, CIFRAS SIMÉTRICAS, APLICAÇÕES DE CONTEÚDOS MATEMÁTICOS E MUITAS OUTRAS CURIOSIDADES.

"Dissertação apresentada ao Centro de Ciências e Tecnologia da Universidade Estadual do Norte Fluminense Darcy Ribeiro, como parte das exigências para obtenção do título de Mestre em Matemática."

Orientador: Prof. Mikhail Petrovich Vishnevski

UNIVERSIDADE ESTADUAL DO NORTE FLUMINENSE
DARCY RIBEIRO - UENF
CAMPOS DOS GOYTACAZES - RJ
OUTUBRO DE 2016

FICHA CATALOGRÁFICA

Preparada pela Biblioteca do **CCT** / **UENF** **187/2016**

Santos, Ana Paula Ferreira dos

A criptografia no ensino fundamental II : contexto histórico, cifras simétricas, aplicações de conteúdos matemáticos e muitas outras curiosidades / A na Paula Ferreira dos Santos. – Campos dos Goytacazes, 2016.

130 f. : il.

Dissertação (Mestrado em Matemática) -- Universidade Estadual do Norte Fluminense Darcy Ribeiro. Centro de Ciência e Tecnologia. Laboratório de Ciências Matemáticas. Campos dos Goytacazes, 2016.

Orientador: Mikhail Petrovich Vishnevski.

Área de concentração: Criptografia.

Bibliografia: f. 75-76.

1. CRIPTOGRAFIA 2. CRIPTOGRAFIA – HISTÓRIA 3. CIFRAS SIMÉTRICAS I. Universidade Estadual do Norte Fluminense Darcy Ribeiro. Centro de Ciência e Tecnologia. Laboratório de Ciências Matemáticas II. Título

CDD 652.8

ANA PAULA FERREIRA DOS SANTOS

A CRIPTOGRAFIA NO ENSINO FUNDAMENTAL II: CONTEXTO HISTÓRICO, CIFRAS SIMÉTRICAS, APLICAÇÕES DE CONTEÚDOS MATEMÁTICOS E MUITAS OUTRAS CURIOSIDADES.

"Dissertação apresentada ao Centro de Ciências e Tecnologia da Universidade Estadual do Norte Fluminense Darcy Ribeiro, como parte das exigências para obtenção do título de Mestre em Matemática."

Aprovada em 25 de Outubro de 2016.

Profª. Adriana Pimenta de Figueiredo
D.Sc. - UNIRIO

Prof. Oscar Alfredo Paz La torre
D.Sc. - UENF

Prof. Nelson Machado Barbosa
D.Sc. - UENF

Prof. Mikhail Petrovich Vishnevski
D.Sc. - UENF
(ORIENTADOR)

Dedico este trabalho à minha falecida e amada mãe, a quem devo tudo que sou. É a principal referência de mulher forte, determinada e otimista, sobretudo de muita fé e que, sozinha, ensinou-me o essencial, preparando-me para que, com dignidade, soubesse contornar as vicissitudes ao longo da caminhada. Infelizmente, não pôde participar dessa etapa de minha vida, e esta é a melhor homenagem que poderia prestar-lhe, como fruto de seus sábios ensinamentos. Peço-lhe perdão pelas minhas ausências, na certeza de sua compreensão. Te amo, mãe.

Agradecimentos

A Deus em primeiro lugar, pela força necessária para que enfrentasse todos os obstáculos, por não permitir que desistisse, por colocar em meu caminho tantas pessoas maravilhosas e fundamentais para o meu crescimento e desenvolvimento pessoal e profissional. Sem a minha fé e o Seu amor nada conseguiria.

A João Victor e Anna Clara, amados filhos, pela compreensão de minha ausência nos diversos momentos em que trabalhava ou estudava, bem como pela paciência com o estresse em decorrência das preparações para as provas e apresentações.

A Zenilda e Luciane, amadas tia e prima, pelas orações e apoio logístico no que concerne aos filhos, garantindo-me o tempo de estudo e pesquisa. Sem vocês esse sonho jamais seria possível.

A minha família PROFMAT, ao tornar mais alegres os sábados durante o curso, corroborando o valor da união, incentivando nas fases de esgotamento físico e mental. Ficará para sempre na memória e no coração.

Ao meu orientador Mikhail e demais professores, que sempre se mostraram atenciosos, preocupados e dispostos. Sem dúvida, exemplos de profissionais.

A todos os amigos que, de forma direta ou indireta, me incentivaram e apoiaram, através de gestos, palavras ou orações. São tantos que não tenho como mencionar um por um.

A minha falecida mãe, a quem devo minha existência e excelente criação. De onde estiver, estará orgulhosa com o meu desempenho e conquista.

"O impulso para descobrir segredos está profundamente enraizado na natureza humana."

(John Chadwick)

Resumo

Neste trabalho, temos como objetivo propor atividades que façam uso do estudo da criptografia e das cifras simétricas como mais uma opção de material de trabalho para o professor de Matemática do segundo segmento do Ensino Fundamental, visando ajudar o docente a estimular a aprendizagem e despertar o interesse dos alunos pela disciplina. Para utilizar a criptografia, devemos saber o que é, como funciona e conhecer sua história e, para auxiliar o professor nessa parte, fizemos um breve resumo sobre a história da criptografia. Citamos seus principais momentos, esclarecemos e exemplificamos diversos tópicos como, por exemplo, as cifras simétricas de substituição, transposição, monoalfabéticas e polialfabéticas. Abordamos, de forma sucinta, as principais teorias de aprendizagem formuladas até os dias de hoje. Esse estudo foi de extrema importância na elaboração das atividades propostas, pois contribuiu para uma melhor compreensão do processo de ensino e aprendizagem da matemática. Nas atividades propostas, fizemos uma conexão entre a criptografia, o processo de ensino da matemática e alguns conteúdos matemáticos a serem trabalhados no ensino fundamental. Finalizamos defendendo a ideia de que a criptografia pode ser utilizada como mais um método de estímulo para desenvolver no aluno o gosto pela matemática, aperfeiçoando o seu raciocínio lógico, ensinando-o a pensar matematicamente por meio de situações interessantes e motivantes.

Palavras-chaves: Criptografia. História da Criptografia. Cifras Simétricas.

Abstract

In this work, we aim to propose activities that make use of ciphers and symmetric ciphers as another work option for the mathematics teacher in 6^{th} to 9^{th} grade, aiming to help teachers to stimulate learning and encourage students' interest in the discipline. To use encryption, we should know what it is, how it works and know its history, and to assist the teacher in this part, we made a brief summary of the history of cryptography. We quote his key moments, clarify and illustrate the various topics such as, for example, symmetrical substitution ciphers, transposition, monoalphabetic and polyalphabetic. We briefly approach, the main learning theories formulated up to the present days. This study was extremely important for the development of the proposed activities, it contributed to a better understanding of teaching and learning mathematics process. In the proposed activities, we made a connection between the encryption, the mathematical teaching process and some mathematical contents to be worked in elementary school. We finished defending the idea that encryption can be used as another method useful to stimulate in the student a taste for mathematics, improving his logical thinking, teaching him how to think mathematically through interesting and challenging situations.

Key-words: Cryptography. History of Cryptography. Symmetric Ciphers.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

PCN	Parâmetros Curriculares Nacionais

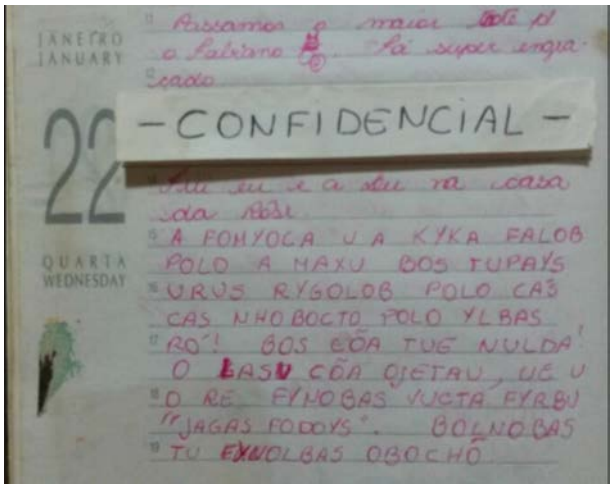
Sumário

Introdução

> Desde a troca de mensagens apaixonadas num caso de amor proibido até informações secretas e vitais para a sobrevivência de povos e nações, sempre houve e sempre haverá motivos para a existência de segredos. Seja por conveniência ou por necessidade, as formas de ocultação acabam sendo tão inocentes ou geniais, tão simples ou repletas de truques quanto a imaginação e a criatividade do ser humano. (TKOTZ, 2005, p.24)

Ainda na adolescência, muito antes de pensar em me graduar em Matemática, lembro-me de que eu e minhas amigas conversávamos utilizando a língua do "p"[1] ou a língua do "i"[2] para que ninguém pudesse entender o que falávamos. Depois de um tempo, esse artifício começou a ficar muito conhecido e, portanto, perdeu sua utilidade. Começamos então a inventar formas secretas para escrever mensagens umas para as outras ou para escrever em nossos diários (Figura 1), era uma forma segura de garantir que nossos segredos ficariam somente entre nós.

Figura 1 – Mensagem criptografada pela autora em sua agenda de 1992



Fonte: Elaborado pela autora

Utilizávamos uma lógica que só nós conhecíamos, trocávamos as letras da mensagem original por outras letras do alfabeto. Sem sabermos, estávamos usando a criptografia e, levando em conta nossa falta de conhecimento do assunto, éramos excelentes criptógrafas.

[1] Consiste em repetir, após cada sílaba, a mesma sílaba trocando a consoante inicial pela letra "p" ou acrescentando "p" ao início da sílaba caso iniciasse com vogal.

[2] Consiste em substituir todas as vogais por "i".

Os meninos da escola ficavam muito curiosos e tentavam decodificar nossas mensagens. Alguns quase conseguiam, descobriam uma letra ou outra observando a frequência com que apareciam nas mensagens. De forma intuitiva, estavam fazendo mentalmente uma análise de frequência mas nunca obtiveram sucesso, eram péssimos criptoanalistas.

A criptografia é uma palavra de origem grega. Cripto (do grego kryptos) significa ocultar e grafia (do grego graphein) significa escrever. Então criptografia seria a escrita oculta ou escrita secreta. A palavra "análise" significa investigar, logo entende-se que criptoanálise é investigar coisas ocultas, claro que com intuito de desvendar o que está oculto. Somente há cerca de vinte anos que a criptografia e a criptoanálise começaram a ser estudadas como uma ciência, antes eram consideradas uma arte. Juntas elas formam uma ciência chamada Criptologia. (TKOTZ, 2005, p. 16)

Segundo TKOTZ (2005), "A criptologia se ocupa da *ocultação* de informações e da *quebra dos segredos* de ocultação, aquela é chamada de criptografia, e esta de criptoanálise". A criptografia está diretamente ligada à necessidade de se guardar informações com segurança e a criptoanálise à necessidade de descobrir essas informações. O desenvolvimento desses dois ramos da criptologia está diretamente ligado ao avanço tecnológico até os dias de hoje.

Na figura 2 temos um esquema de ramificação da criptologia que organiza os principais tópicos dessa ciência. Embora seja um assunto muito interessante, não cabe aqui um estudo de todo seu conteúdo, já que o mesmo seria demasiadamente extenso. Sendo assim, escolhemos um ramo dessa ciência que mais nos atraiu para aplicação em sala de aula no ensino fundamental: a criptografia e o estudo das cifras simétricas. A criptoanálise, a esteganografia, os códigos e as cifras assimétricas serão mencionados, mas apenas como forma de enriquecimento teórico, para melhor estruturar o trabalho.

Figura 2 – Áreas da Criptologia

Fonte: Elaborado pela autora

Inspirados não somente pelas agradáveis lembranças de escola, bem como pelo

aspecto moderno, atrativo e de extrema aplicabilidade matemática, escolhemos a criptografia como tema principal.

Existem muitos problemas enfrentados pelos professores no exercício da sua função. Um dos maiores, concernente ao professor de matemática, é a dificuldade dos alunos na aprendizagem significativa da disciplina.

É comum o professor de matemática ser questionado por seus alunos quanto à necessidade de aprender certos conteúdos. Questionamentos e reclamações a respeito do uso da Matemática e das dificuldades de compreender e assimilá-la são muito frequentes. A visão pessimista do aluno, a falta de interesse pela Matemática, assim como a desmotivação de estudar, são situações corriqueiras na sala de aula e que dificultam ainda mais o trabalho do professor. O que acarreta tudo isso? Os motivos são diversos, desde financeiros a psicológicos, mas não podemos fugir da nossa responsabilidade como parte desse problema. Professores desatualizados, desestimulados, cansados e sem tempo, contribuem para esse quadro catastrófico. Temos conhecimento de todos os transtornos enfrentados pela classe. Ainda assim, não podemos permitir que esses problemas gerem mais problemas. O professor precisa se atualizar, buscar alternativas para tornar suas aulas mais dinâmicas e atrativas, abordar assuntos diferentes e atuais, enfim, tentar minimizar a dificuldade de aprendizagem do aluno.

Consta no PCN que "a aquisição do conhecimento matemático deve estar vinculada ao domínio de um saber fazer matemática e de um saber pensar matemático" (BRASIL, 1998, p. 41). O estudo da criptologia não está no currículo mínimo da educação básica, contudo tanto a criptografia quanto a criptoanálise podem ser introduzidos dentro de conteúdos já existentes no currículo e com a grande vantagem de não necessitarem, como requisito, de conhecimentos matemáticos avançados e, em alguns casos, não necessitam de nenhum conhecimento matemático. Podem ser muito úteis no processo de ensino e aprendizagem da matemática, como ferramenta de motivação nas aulas, tornando-as mais interessantes, dinâmicas e atuais. Dessa forma, ajudando a desenvolver o pensar e o saber matemático, estimulando o raciocínio lógico do aluno e sua criatividade.

> Para tanto, é importante que a Matemática desempenhe, equilibrada e indissociavelmente, seu papel na formação de capacidades intelectuais, na estruturação do pensamento, na agilização do raciocínio dedutivo do aluno, na sua aplicação a problemas, situações da vida cotidiana e atividades do mundo do trabalho e no apoio à construção de conhecimentos em outras áreas curriculares. (BRASIL, 1998, p. 25)

Pesquisando sobre o tema, verificamos a existência de poucos trabalhos sobre criptografia aplicada ao processo de ensino da matemática no ensino fundamental. Talvez o motivo dessa carência de material esteja ligado ao fato da criptografia não fazer parte do currículo mínimo das escolas. Mas isso não nos desanimou em nenhum momento,

pelo contrário, foi mais um fator motivacional para o desenvolvimento deste trabalho. As dissertações dos professores LOUREIRO (2014), MATSUMOTO (2014) e FIARRESGA (2010) foram de extrema importância como fonte de pesquisa e inspiração. Inclusive, a decisão de abordar o tema com foco no ensino fundamental, foi para complementar a pesquisa realizada e defendida nessa instituição de ensino pelo professor LOUREIRO (2014). É importante ressaltar que, embora o tema principal seja o mesmo, as pesquisas se diferem quanto ao público alvo, aos objetivos e a estrutura das atividades.

Nosso objetivo geral é propor atividades para sala de aula que utilizam o estudo da criptografia e das cifras simétricas no ensino fundamental. Essas atividades são uma opção de material que abordam um assunto diferente e atual, visando facilitar o trabalho do docente, estimular a aprendizagem e despertar o interesse do aluno pela Matemática.

Para atingir nossos objetivos, estruturamos esse trabalho em quatro capítulos. O primeiro capítulo aborda a história da criptografia. Afinal, saber como surgiu, assim como sua utilização ao longo da história, é fundamental para o professor fazer um bom trabalho com seus alunos em sala de aula. O contexto histórico de um conteúdo e a sua aplicação no cotidiano é muito importante no processo de ensino e aprendizagem, pois além de humanizar a matemática, aproximando-a cada vez mais da realidade do aluno, ajuda-nos a entender a sua importância para a humanidade, como também, o seu desenvolvimento ao longo do tempo.

No capítulo dois, faremos um resumo dos principais conceitos pedagógicos que envolvem o processo de ensino e aprendizagem da Matemática. Abordaremos algumas teorias importantes que foram responsáveis pela evolução do processo educacional, além de mencionar temas como inteligências múltiplas e aprendizagem significativa. Como o objetivo das atividades propostas neste trabalho é estimular o gosto pela Matemática utilizando a criptografia, almejando uma aprendizagem mais significativa, esse estudo nos ajudou a compreender como o aluno aprende e como esse processo ocorre biológica e emocionalmente. Sem dúvida, além de esclarecedor e interessante, foi também muito importante para a estruturação das atividades e deste trabalho como um todo.

Toda pesquisa deve seguir uma linha de raciocínio, um conjunto de procedimentos intelectuais e técnicos para que os objetivos sejam atingidos. A metodologia de pesquisa utilizada para conduzir esse trabalho foi tratada no capítulo três.

Então, depois de bem fundamentados os conceitos históricos da criptografia e teóricos da aprendizagem, teremos no quarto capítulo o produto de todo esse estudo, que são as atividades que utilizam a Criptografia e as cifras simétricas para serem aplicadas a partir do sexto ano do ensino fundamental.

Para finalizar, analisamos de uma forma geral o que foi desenvolvido durante esse trabalho, propondo uma continuidade do mesmo.

Capítulo 1

Um pouco de história

Neste capítulo, faremos um breve resumo sobre a história da criptografia. Abordaremos as partes que mais serão úteis nas aplicações das atividades propostas no quarto capítulo. Embora exista muita aplicação matemática na criptografia, principalmente utilizando conteúdos do Ensino Médio e, diga-se de passagem, que foram muito bem trabalhados pelo professor LOUREIRO (2014) em sua dissertação, é importante ressaltar que nosso público alvo são alunos do ensino fundamental. Nosso objetivo é fornecer ao professor de matemática conhecimento histórico do tema para que ele promova o entendimento ao educando de como a Matemática fez parte de grandes acontecimentos históricos e, ainda hoje, é responsável por muitos avanços na área tecnológica. Este pode ser um caminho para que o aluno se interesse mais pelos conteúdos matemáticos, vença barreiras no processo de aprendizagem e, assim, modifique a sua história de vida. (MATSUMOTO, 2014, p. 1)

> A necessidade de se proteger uma informação é antiga. No início, a criptografia era uma ferramenta usada exclusivamente por governos em situações de guerra ou quando desejassem manter uma comunicação segura ou proteger alguma informação vital, que poderia causar danos se caísse em mãos inimigas. E, assim foi por milhares de anos, até a invenção dos computadores e da internet. Hoje a criptografia não é mais uma ciência de uso quase que exclusivamente militar. Não só os governos que precisam proteger informações, empresas e pessoas necessitam da criptografia para proteger suas informações. (LOUREIRO, 2014, p. 1)

Atualmente vivenciamos a era tecnológica. Estamos conectados vinte quatro horas por dia através de redes de comunicação via internet, jornal, televisão, rádio, enfim, a informação é extraordinariamente veloz. Precisamos nos adaptar a essa realidade e utilizar toda essa tecnologia a nosso favor. Todos esses aparelhos, tão reverenciados por alunos e professores, podem se tornar ferramentas importantes no processo de aprendizagem da matemática.

Sabemos que, sem a matemática, não existiria a realidade tal qual é. As pessoas

não têm noção do quanto gostam da matemática, ou pelo menos, do quanto gostam do que essa ciência lhes proporciona. Com o avanço da tecnologia, o mundo ficou menor, perdeu fronteiras, encurtou distâncias. Isso foi muito bom por um lado mas, por outro, gerou sérios problemas.

Estamos muito expostos nos dias de hoje. Qualquer pessoa pode obter informações sobre nossa vida; aos nossos dados pessoais, profissionais ou até mesmo bancários; caso estes não estejam devidamente protegidos. A maioria das informações está aberta a todos, mas há aquelas que não podem estar abertas para todos, são informações sigilosas que pertencem a uma determinada pessoa ou a um limitado grupo de pessoas. Informações bancárias, senhas, projetos de trabalho, tudo hoje em dia fica guardado em nossos computadores e essas informações, se interceptadas, podem causar grandes transtornos (MATSUMOTO, 2014, p. 4). Existe então uma necessidade, que é instintiva do ser humano, que é a de proteção. Guardar informações particulares é uma forma de se proteger.

1.1 O que é a criptografia

Antes de conhecermos um pouco da história da criptografia precisamos entender melhor o que é a criptografia.

> 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 certos assuntos é a vontade dos mesmos humanos em desvendar esses segredos. Sejam segredos individuais ou coletivos. (MATSUMOTO, 2014, p. 4)

A criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada de um texto claro[1] para um texto cifrado[2], de forma que possa ser conhecida apenas por seu destinatário, detentor da chave[3], o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

A criptografia tem utilizado diferentes cifras[4] ao longo do tempo. Existem as cifras simétricas e as assimétricas. As simétricas são aquelas que utilizam a mesma chave secreta para cifrar e decifrar mensagens. São muito úteis e rápidas mas não são muito seguras (TKOTZ, 2005, p. 238). Foram criadas muitas dessas cifras simétricas na História, mas iremos citar somente algumas delas, aquelas que serão utilizadas nas propostas de atividades desse trabalho. Já as cifras assimétricas possuem dois tipos de chaves: uma

[1] Como chamamos a mensagem na sua forma original.
[2] Como chamamos a mensagem transformada para uma forma ininteligível.
[3] É o nome que damos a uma espécie de senha (que pode ser número, letra, palavra, frase) que dá início ao processo de cifragem.
[4] Métodos para criptografar.

pública e outra privada. A primeira é usada para cifrar a mensagem e a segunda para decifrar, sendo apenas do conhecimento do receptor da mensagem. As cifras assimétricas possuem muita aplicação matemática baseada na teoria dos números, um conteúdo muito importante e interessante para nós professores, mas é extremamente difícil e fora da realidade dos alunos do ensino fundamental. Por esse motivo, abordaremos apenas com a finalidade de aguçar a curiosidade destes alunos sobre o tema e como enriquecimento teórico para os professores.

As cifras simétricas podem ser de substituição ou de transposição. Na cifra de transposição cada letra conserva a sua identidade, mas muda de posição dentro da mensagem, enquanto na cifra de substituição, cada letra conserva a sua posição, mas é substituída por uma outra letra ou símbolo (FIARRESGA, 2010, p. 4). Também foram muito utilizadas, e são até hoje, cifras que misturam mais de um método de cifragem, chamadas de supercifragem, dificultando muito a decodificação, tornando essa forma de cifragem muito mais segura.

Para codificarmos um texto claro utilizando o método da substituição, um dos primeiros passos é fazer corresponder o alfabeto comum a um alfabeto em cifra. Nas cifras de substituição monoalfabéticas, que foram bastante eficientes durante séculos, o alfabeto simples é reordenado, substituído por números ou outros caracteres, criando desta forma uma correspondência biunívoca. Após escrevermos o texto claro, substituímos cada letra, pela letra ou símbolo correspondente do alfabeto em cifra, criando um texto cifrado que somente será entendido pelo seu verdadeiro destinatário, possuidor da chave. Esse tipo de cifra hoje em dia é facilmente decifrável por uma análise de frequência das letras do alfabeto da língua em questão, o que a tornou inútil diante dos propósitos da criptografia. A quebra das chaves das cifras de substituição monoalfabéticas, através da análise de frequências, levou ao surgimento das cifras de substituição polialfabéticas. Neste tipo de cifragem utilizam-se diversos alfabetos de cifra, ou seja, na passagem do texto claro para o texto cifrado cada uma das letras pode ser substituída ao longo da mensagem por diversas letras ou símbolos, com chaves diferentes, dificultando a decifragem da mensagem pela análise de frequência. (FIARRESGA, 2010, p. 5)

Antigamente, a cifragem era utilizada em três situações específicas: na troca de mensagens de estratégias de guerra, com intuito de o inimigo não descobrir as estratégias, caso se apoderasse dela; no amor, para que os segredos amorosos não fossem descobertos pelos familiares; e à diplomacia, para que facções rivais não estragassem os planos de acordos diplomáticos entre nações. Atualmente os objetivos da criptografia continuam sendo ligados a privacidade de informações mas com muito mais segurança. Segundo (FIARRESGA, 2010, p. 4), os objetivos da criptografia são:

- Confidencialidade – mantém o conteúdo da informação secreto para todos exceto para as pessoas que tenham acesso à mesma.

- Integridade da informação – assegura que não há alteração, intencional ou não, da informação por pessoas não autorizadas.
- Autenticação de informação – serve para identificar pessoas ou processos com quem se estabelece comunicação.
- Não repudiação – evita que qualquer das partes envolvidas na comunicação negue o envio ou a recepção de uma informação.

Ao longo da história, muitas cifras foram criadas com intuito de guardar informações e foram realmente úteis durante algum tempo. Tiveram papéis importantes em muitos fatos históricos mas depois de quebradas, perderam totalmente a sua utilidade. Com o avanço tecnológico, foram criadas as máquinas de cifragem cujos textos cifrados eram impossíveis de serem decifrados manualmente, pois permitiam um número enorme de possibilidades de chaves. Logo depois vieram os poderosos computadores e, com eles, a necessidade de guardar informações aumentou ainda mais. Atualmente a criptografia conta com cifras muito avançadas que garantem, pelo menos por enquanto, a segurança das informações transmitidas.

1.2 A escrita sagrada

A criptografia é extremamente interessante e moderna. Entretanto, embora tenha um aspecto atual, não teve início nos tempos de hoje. O interesse do homem pela criptografia é muito mais antigo do que se imagina. A escrita hieroglífica é o primeiro indício histórico da preocupação do homem em tornar textos ininteligíveis.

Não é a toa que quando alguém tem uma letra muito difícil de entender é comum ouvirmos brincadeiras e críticas, comparando a escrita com hieróglifos. A impressão é que a pessoa escreve através de códigos impossíveis de serem decifrados, verdadeiros enigmas. Hieróglifo ou hieroglifo é cada um dos sinais da escrita de antigas civilizações, tais como os egípcios, os hititas, e os maias. É um termo originário de duas palavras gregas: hierós "sagrado", e glýphein "escrita".

Uma curiosidade a respeito disso data-se de 2000 a.C., no Antigo Egito. "Numa vila egípcia perto do Nilo, chamada Menet Khufu, o escriba responsável pelas inscrições do túmulo de Khnumhotep II resolveu dar uma caprichada e substituiu alguns hieróglifos por outros que ele considerava mais refinados, adequados à importância do falecido" (TKOTZ, 2005, p. 17). Foram usados hieróglifos que não eram compreendidos pelo resto da população. Embora o objetivo do escriba não tenha sido de esconder segredos, essa troca de símbolos pode ser considerada a primeira criptografia de substituição da história.

Figura 3 – Hieróglifos em uma estela funerária

Fonte: www.instrublu.blogspot.com.br/2014/05/principios-da-leitura-de-hieroglifos.html

Embora fosse de difícil compreensão, a escrita hieroglífica (Figura 3) não é necessariamente criptográfica. Já que a grande maioria das pessoas da época era iletrada, elas não tinham mesmo condições de entender os símbolos e seus significados. Apenas os sacerdotes, membros da realeza, altos cargos, e escribas conheciam a arte de ler e escrever esses sinais "sagrados".

Algumas fontes atribuem aos chineses a origem da escrita secreta mas a maioria não considera a escrita logográfica chinesa como criptográfica. Estima-se ter surgido antes mesmo da Dinastia Shang, aproximadamente 2000 a.C, e assim como no antigo Egito, a escrita era uma atividade da minoria letrada, portanto, naturalmente secreta. (TKOTZ, 2005)

A criptografia não apareceu somente num determinado local. Foi aparecendo em diferentes civilizações, de diversos modos, e todas com o mesmo objetivo - guardar o significado da mensagem.

1.3 Criptografar ou esconder?

A escrita secreta começou a ser conhecida pelo relato feito por Heródoto, um historiador romano, por volta do século V antes de Cristo, que relatou em sua obra “As Histórias” os conflitos ocorridos entre a Grécia e Pérsia.

Herótodo escreveu que foi a arte da escrita secreta que salvou a Grécia de ser

conquistada por Xerxes, o déspota líder dos Persas. Xerxes passou cinco anos montando secretamente a maior força de combate da história mas ele não contava que, simultaneamente, a Grécia, que já tinha descoberto suas intenções de ataque surpresa, já se preparava para o combate.

Foi o grego Demerato, que morava na Pérsia, que enviava mensagens secretas à Grécia. Ele escrevia em um par de tabuletas raspando a cera e depois a escrita era coberta novamente para assim ser passada pelos guardas sem ser descoberta. Com isso em 480 a.C. Xerxes, líder dos Persas, atacou a Grécia mas, ao invés de surpreender ele que foi surpreendido. Os gregos os aguardavam bem preparados e, graças a estratégia de Demerato, venceram a guerra.

Ainda em “As Histórias”, Heródoto relata a história de Histaeu, que para enviar uma mensagem secreta a Aristágora, raspou a cabeça de um mensageiro, escreveu a mensagem no couro cabeludo e esperou o cabelo crescer. O mensageiro, que aparentemente não levava nada que fosse perigoso, chegou ao destinatário e raspou a cabeça, revelando a mensagem. (TKOTZ, 2005)

A arte de esconder uma mensagem, sem nenhum tratamento para modificá-la, e uma técnica primitiva chamada esteganografia, que deriva do grego Steganos, coberto, e graphia, escrita. Apesar de primitiva, a longevidade da esteganografia demonstra que ela oferece certa segurança, entretanto trata-se de um procedimento sem fundamento científico.

Durante a Segunda Guerra Mundial, agentes alemães que atuavam na América Latina, utilizaram uma técnica de transmissão de mensagem que consistia em microfilmar uma página de texto, reduzindo ao tamanho de um ponto. Este ponto era colocado sobre um ponto final de um documento aparentemente inofensivo. O receptor, ao receber a mensagem, procurava pelo ponto e ampliava-o para ter acesso a informação. Os aliados descobriram a técnica em 1941 e passaram a interceptar a comunicação. A principal deficiência deste tipo de técnica é que, caso a mensagem seja descoberta, poderá ser lida por qualquer pessoa.

A esteganografia é um ramo da Criptologia e, paralela ao seu desenvolvimento, houve a evolução da criptografia. Esse ramo da matemática tem algo de misterioso e excitante, sua história é recheada de acontecimentos intrigantes, tanto que já inspirou inclusive muitos filmes e livros.

Apesar da distinção entre esteganografia e criptografia, é possível utilizar um sistema que englobe as duas técnicas, onde uma mensagem é criptografada e o texto ininteligível é escondido, como no episódio em que um texto era transformado em um ponto, durante a segunda guerra mundial. Após a descoberta dos aliados, os alemães passaram a tomar a precaução extra de criptografar a mensagem antes de microfilmá-la.

1.4 Cítala ou bastão de Licurgo

No século V a.C. os gregos antigos, e em particular os espartanos, utilizaram este sistema de cifra de transposição para se comunicar nas batalhas militares.

Neste cilindro, era enrolada uma tira de couro ou papiro, onde era escrita uma mensagem no sentido do seu comprimento, em seguida desenrolava-se a tira e era transportada como um cinto, com as letras voltadas para dentro, por um mensageiro até ao destinatário. Este enrolava a tira num bastão de igual diâmetro e ficava conhecedor de tão importante informação.

Figura 4 – Cítala ou bastão de Licurgo

Fonte: https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-em-python/

Com a Cítala (Figura 4), os governantes e generais de Esparta trocavam, com segurança, as suas mensagens secretas.

1.5 As cifras de substituição monoalfabéticas

Entre 600 a.C. e 500 a.C., as três cifras hebraicas Atbash, Albam e Atbah, como podemos ver na figura 5, eram as mais conhecidas e usadas principalmente em textos religiosos.

Figura 5 – As cifras hebraicas

Atbash

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
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	A

Albam

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
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

Atbah

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

Fonte: slideplayer.com.br/slide/395343

Um fato interessante sobre a cifra de Atbash é que escribas hebreus usaram-na para escrever algumas palavras do Livro de Jeremias. Atbash é uma criptografia de simples substituição do alfabeto hebraico. Ela consiste na substituição da primeira letra pela última, da segunda letra pela penúltima, e assim por diante, invertendo o alfabeto usual.

Exemplo 1 *Utilizando a cifra de Atbash, vamos criptografar a palavra PROFMAT.*

A primeira letra do texto claro é P e será substituída por K, a segunda letra do texto claro é R e será substituída por I, e assim por diante. Veja o resultado na tabela 1:

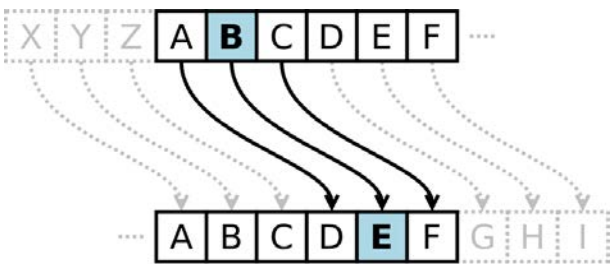
Tabela 1 – Cifragem utilizando a cifra de Atbash

TEXTO CLARO	P	R	O	F	M	A	T
TEXTO CIFRADO	K	I	L	U	N	Z	G

Segundo (TKOTZ, 2005), os indianos eram também grandes conhecedores das formas de comunicação secreta. Temos como exemplo o Kama-Sutra, um antigo texto indiano datado do século IV, escrito pelo estudioso brâmane Vatsyayana, baseado em manuscritos que datam de 400 a.C., que recomenda às mulheres estudarem 64 artes, incluindo culinária, vestuário, massagem, fabricação de perfumes e a arte da escrita secreta, justificada de modo a ajudar as mulheres a esconderem os detalhes de seus relacionamentos. A técnica consistia em um aparelhamento ao acaso das letras do alfabeto, substituindo-se cada letra na mensagem original por seu par.

A criptografia mais conhecida, a primeira com propósitos militares, surgiu nas Guerras da Gália de Júlio César, e por este motivo ficou conhecida como Cifra de César (Figura 6). Ele substituía cada letra na mensagem por outra que estivesse três casas à frente no alfabeto. Apesar de simples e facilmente quebrável, a Cifra de César parece ter tido grande sucesso em sua época, visto ser analfabeta a maioria dos inimigos do Império Romano, e os poucos que sabiam ler imaginavam que o texto estivesse escrito em outra língua. No entanto, após ter sido descoberta a chave perdeu sua funcionalidade.

Figura 6 – A cifra de César



Fonte: canaltech.com.br/o-que-e/protecao-de-dados/o-que-e-criptografia-e-por-que-voce-deveria-usa-la/

Exemplificando a lógica deste método, em um texto criptografado com chave 3, cada letra aumentaria em três posições no alfabeto: 'A' se tornaria 'D', 'B' se tornaria 'E' e

assim por diante. Chegando ao final do alfabeto, ele retornaria ao início, por exemplo, 'Z' se tornaria 'C'. A figura abaixo ilustra melhor esta troca.

Exemplo 2 *Utilizando a cifra de César, vamos criptografar a palavra CIFRA.*

Na primeira linha temos o alfabeto normal e, na segunda linha, temos o alfabeto deslocado três casas à direita. Veja a figura 7:

Figura 7 – Cifragem utilizando a Cifra de César

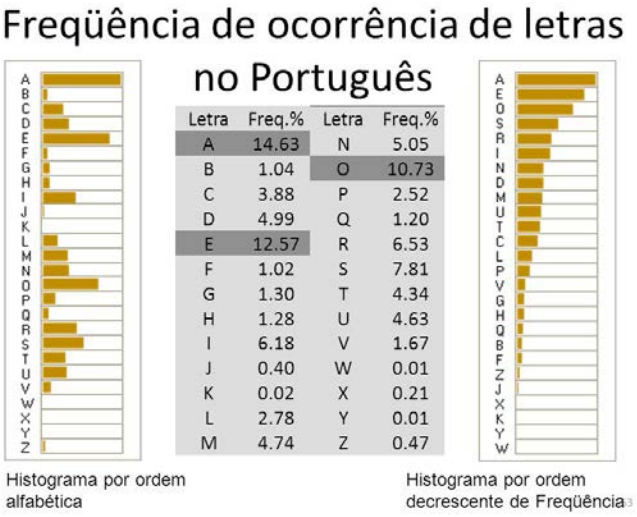
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: pt.slideshare.net/anchises/criptografia-simetria-e-assimtrica

Sendo assim, utilizando a cifra de César, a palavra CIFRA seria transformada em FLIUD.

Ao trabalharmos com nossos alunos essas cifras de substituição simples, seja a de César, de Atbash ou qualquer outra, não podemos deixar de mencionar o motivo pelo qual tornaram-se inúteis. A facilidade de se decifrar mensagens de substituição monoalfabética, utilizando análise de frequência (Figura 8), é relativamente simples.

Figura 8 – Análise de Frequência na língua portuguesa



Letra	Freq.%	Letra	Freq.%
A	14.63	N	5.05
B	1.04	O	10.73
C	3.88	P	2.52
D	4.99	Q	1.20
E	12.57	R	6.53
F	1.02	S	7.81
G	1.30	T	4.34
H	1.28	U	4.63
I	6.18	V	1.67
J	0.40	W	0.01
K	0.02	X	0.21
L	2.78	Y	0.01
M	4.74	Z	0.47

Fonte: sideplayer.com.br/slide/383339

A análise de frequência em uma determinada língua consiste na frequência em que cada letra ou palavra, da língua em questão, aparece em um texto. Quanto maior o texto, mais exata é a frequência de cada letra ou palavra. É uma ótima oportunidade de trabalhar porcentagem, mas com cuidado, para não ser muito cansativo.

Um exemplo dessa fragilidade nas cifras de substituição foi a tragédia que ocorreu com a rainha da Escócia Mary Stuart (1542-1587). Prisioneira da rainha Elizabeth I por 18

anos, Mary I conspirava em cartas cifradas, utilizando símbolos no lugar das letras e palavras. As cartas eram interceptadas por Francis Walsingham, espião a serviço da coroa britânica, e foram facilmente decifradas pelo melhor criptoanalista da época, Thomas Phelippes. Mary Stuart foi descoberta, condenada por conspiração e decapitada em 1587.(TKOTZ, 2005)

1.6 O disco de Alberti e a cifra de Vigenére: o surgimento das cifras polialfabéticas

Leon Battista Alberti, em 1466, foi um dos primeiros a projetar e usar um dispositivo que facilitava o processo criptográfico. Este dispositivo ficou conhecido como Disco de Alberti.

Figura 9 – Disco de Alberti

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

O disco de Alberti (Figura 9), é composto por dois anéis concêntricos, um externo e um interno. O anel externo é fixo, com 24 casas contendo 20 letras latinas maiúsculas (incluindo o Z, com U=V e excluindo H J K W Y) e os números 1, 2, 3, e 4 para o texto claro. O anel interno é móvel, com as 24 letras latinas minúsculas para o texto cifrado. As 20 letras maiúsculas estão em ordem alfabética e as 24 minúsculas estão desordenadas. Letras minúsculas fora de ordem é uma norma fundamental pois, caso estivessem em ordem, a cifra seria apenas uma generalização do Código de César. (TKOTZ, 2005, p, 194)

Fabricar o disco de Alberti com os alunos é uma atividade fantástica por, simultaneamente, propiciar o trabalho com círculo, circunferência, ângulo e ainda aplicar a codificação e decodificação de mensagens como um agradável desafio.

Exemplo 3 *De posse do disco de Alberti, vamos seguir os procedimentos abaixo para cifrar a mensagem "Disco de Alberti":*

1. *Escolhe-se uma letra do disco interno. Esta será a letra-chave. Digamos que a letra escolhida seja p.*

2. *Gira-se o disco interno para alinhar a letra-chave p com uma localizada no disco externo. Para o exemplo, será usada a letra E.*

3. *Inicia-se o criptograma com a letra E para indicar a posição do disco interno (lembre-se que o p é a chave secreta) e as substituições são feitas de acordo com as posições dos dois discos.*

De acordo com esse processo, temos o texto cifrado E nvqly np gzkpmiv.

Até aqui nenhuma diferença em relação a uma substituição simples. Acontece que Alberti sugere trocar o alfabeto cifrante durante o processo de cifragem indicando os pontos de troca pelas letras maiúsculas apontadas pela letra-chave. Assim, se alinharmos a letra p com a letra G, depois de cifrar "Disco de", como mostrado na figura 10, é fácil verificar que a mensagem cifrada final será E nvqly np G ctelsmr.

Figura 10 – Rotações do Disco de Alberti

A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
g	k	l	n	p	r	t	v	z	&	x	y	s	o	m	q	i	h	f	d	b	a	c	e
c	e	g	k	l	n	p	r	t	v	z	&	x	y	s	o	m	q	i	h	f	d	b	a

Fonte: Elaborado pela autora

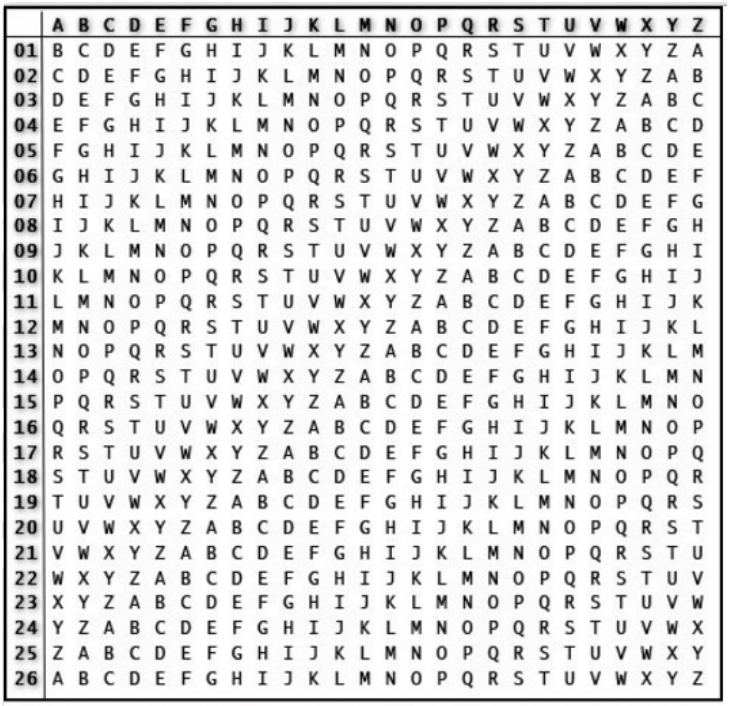
Neste caso, trata-se de uma substituição polialfabética com dois alfabetos, podendo ser utilizado um número ainda maior de cifrantes.

A criptografia por substituição era muito usada, o que tornava conhecido o seu método de cifrar e decifrar, sendo de fácil acesso a descoberta da mensagem criptografada. Com isso surgiu uma nova forma de criptografia feita por substituição criada por Blaise de Vigenère em 1563. O grande mérito do autor desta cifra foi o de aperfeiçoar um método que já tinha sido proposto por outros estudiosos, mas que precisava ser estruturado para oferecer a segurança necessária. Vigenère baseou-se em Alberti e Trithemius, como também em alguns contemporâneos, como Bellaso e Della Porta. (LOUREIRO, 2014, p. 8)

O francês Blaise de Vigenère (1523 - 1596) usou a criptografia como instrumento de trabalho durante anos. Com a idade de 39 anos resolveu abandonar a carreira diplomática e dedicar-se exclusivamente aos estudos. Em 1586 Vigenère publica seu livro de criptologia, o Traité des chiffres où secrètes manières d'escrire, no qual descreve detalhadamente sua cifra de substituição polialfabética monogrâmica (conhecida como Carreiras de Vigenère) porque faz uso de vários alfabetos cifrantes aplicados individualmente aos caracteres da mensagem clara, fazendo uso de chaves que podem ser palavras ou frases.

A figura 11 mostra as carreiras de Vigenère. O cabeçalho da tabela (a linha superior) é o alfabeto e a coluna lateral esquerda mostra o deslocamento dos caracteres. Na linha 0, entra o alfabeto com deslocamento 0; na linha 1 os caracteres são deslocados em uma posição (o alfabeto começa com a letra B); na linha 2 os caracteres são deslocados em duas posições e assim sucessivamente.

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

Fonte: https://danieldonda.wordpress.com/2007/10/31/cifradevigenere-le-chiffre-indechiffrable

Para cifrar a primeira letra do texto claro com a primeira letra da chave, procura-se a letra do texto claro no cabeçalho e a letra da chave na coluna da esquerda. A letra encontrada na intersecção das duas referências será a substituta da letra do texto claro. A segunda letra da chave é a primeira letra do texto claro. Repetindo o processo e percorrendo todo o texto claro, cada uma das sua letras, com exceção da última, servirá como chave para a letra seguinte. (TKOTZ, 2005, p.205)

Exemplo 4 *Utilizando a cifra de Vigenère, vamos cifrar a palavra MATEMATICA. Veja na tabela 2:*

Tabela 2 – Cifragem utilizando as carreiras de Vigenère

TEXTO CLARO	M	A	T	E	M	A	T	I	C	A
CHAVE	G	M	A	T	E	M	A	T	I	C
TEXTO CIFRADO	S	M	T	X	Q	M	T	B	K	C

Fonte: Elaborada pelo autora

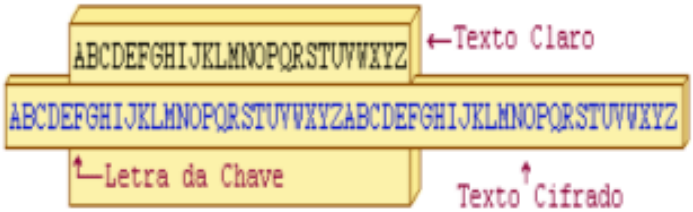
Logo o texto cifrado é SMTXQMTBKC.

O processo de substituição manual é muito sujeito a erros porque a leitura é penosa e, depois de algum tempo, bastante fatigante. Trabalhar com réguas sobre a tabela de alfabetos cifrantes também acaba cansando. Devido a este fato, a partir de 1880, muitos criptólogos passaram a utilizar a chamada Régua de Saint-Cyr (Figura 12).

A segurança da cifra era alta para a época mas hoje é considerada baixa. Foi

somente em 1863 que o criptólogo alemão Kasiski descobriu como quebrar a cifra de Vigenère. O matemático inglês Charles Babbage já havia quebrado a cifra em 1854, fato que ficou desconhecido por muito tempo porque não publicou sua descoberta.

Figura 12 – Régua de Saint-Cyr



Fonte: www.dm.ufscar.br/profs/caetano/iae2004/G6/cifra.htm

1.7 Supercifragem: a cifra ADFGVX

Quando se utiliza mais de um método de cifragem, sejam quais forem esses métodos, para se obter um criptograma, dizemos que foi utilizada uma supercifragem. Uma das supercifragens mais famosas foi a ADFGVX. Essa cifra foi criada pelos alemães no final da Primeira Guerra Mundial. Os alemãs preparavam um ataque final e decisivo mas para isso precisavam de um novo sistema criptológico desconhecido dos aliado e que fosse muito seguro. Os melhores criptógrafos alemãs se reuniram em Berlim e escolheram, entre muitos candidatos, a sua nova arma secreta, o sistema ADFGVX. Esse sistema consiste em uma tabela 6 x 6, onde são colocadas as 26 letras do alfabeto e os algarismos de 0 a 9 (Figura 13). (TKOTZ, 2005)

Figura 13 – A cifra ADFGVX

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	M
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Fonte: slideplayer.com.br/slide/395343

A cifra ADFGVX possui duas etapas de codificação. Para entendermos melhor, vejamos um exemplo:

Exemplo 5 *Vamos codificar a palavra CRIPTOGRAFIA.*

Na primeira etapa, utilizaremos a cifra ADFGVX para codificar letra por letra. Temos que a letra C será substituída por duas letras: F, que indica a linha que está a letra C, e G,

que indica a coluna. Usando o mesmo raciocínio em todo texto claro. Até aí temos uma cifra de substituição monoalfabética e uma análise de frequência seria suficiente para quebrá-la. Veja o resultado na tabela 3:

Tabela 3 – Texto Cifrado

TEXTO CLARO	C	R	I	P	T	O	G	R	A	F	I	A
TEXTO CIFRADO	FG	VV	VG	AD	DD	XG	GV	VV	DV	XV	VG	DV

Fonte: Elaborada pela autora

Texto cifrado: FGVVVGADDDXGGVVVDVXVVGDV

Para a segunda etapa vamos precisar de uma palavra-chave, que deve ser também do conhecimento do destinatário. No nosso exemplo, a palavra-chave é BELA. Vamos montar uma tabela onde a primeira linha deve conter as letras da palavra chave e as demais linhas devem conter as letras do texto cifrado.

Tabela 4 – Palavra-chave e texto cifrado

B	**E**	**L**	**A**
F	G	V	V
V	G	A	D
D	D	X	G
G	V	V	V
D	V	X	V
V	G	D	V

Fonte: Elaborada pela autora

Depois da tabela 4 montada, rearrumamos as colunas de modo que as letras da palavra-chave fiquem em ordem alfabética:

Tabela 5 – Palavra-chave em ordem alfabética

A	**B**	**E**	**L**
V	F	G	V
D	V	G	A
G	D	D	X
V	G	V	V
V	D	V	X
V	V	G	D

Fonte: Elaborada pela autora

Como podemos verificar na tabela 5, o texto cifrado final será: VFGVDVGAGDDXVGVVVDVXVVG

Podemos ver que, na segunda etapa da cifra ADFGVX, é usado o método de transposição, tornando muito mais difícil a criptoanálise do texto cifrado.

Qualquer que seja o texto original, no texto cifrado só aparecerão combinações dessas seis letras A, D, F, G, V e X. As pessoas costumam se perguntar por que logo essas seis letras foram escolhidas e não outras como A. B, C, D, E e F, por exemplo. E a justificativa é muito simples, as mensagens eram transmitidas utilizando o código Morse e essas letras são muito diferentes uma da outra quando traduzidas para os pontos e traços do código Morse, assim as possibilidades de erros durante a transmissão são mínimas. (SINGH, 2001)

1.8 A criptografia e a criptoanálise após a Primeira Guerra Mundial

No final da Primeira Guerra Mundial, em 1918, o alemão Arthur Sherbius (Figura 14) desenvolveu uma nova forma de criptografar.

Figura 14 – Arthur Scherbius

Fonte: www.enigma.umww.pl/index.php?page=Scherbius

Com o objetivo de substituir os sistemas criptográficos ultrapassados usados na Primeira Guerra Mundial, ele construiu uma máquina cifrante que era basicamente uma versão elétrica do disco de Alberti, a qual chamou de Enigma. Aqui se inicia a troca das cifras de papel e lápis por uma mais moderna que utilizava a tecnologia do início do século XX.

A Enigma tinha a aparência de uma máquina de escrever e o modelo mais antigo era composto de três elementos: um teclado para introduzir a mensagem original, uma unidade misturadora para cifrar cada letra da mensagem e um mostrador para visualizar a mensagem cifrada, tudo isso numa caixa de dimensões relativamente reduzidas. Na máquina haviam três misturadores, cada um com vinte e seis possíveis posições, a posição inicial dos misturadores formava a chave da cifra. (TKOTZ, 2005)

Comercialmente a Enigma (Figura 15) foi um fiasco. Mais tarde, outras versões, com algumas alterações, foram finalmente adotadas pela Marinha e depois pelo Exército alemão, obtendo a rede de comunicação mais segura da época. A partir de 1933, modelos da Enigma, diferentes dos modelos comerciais, com configurações super secretas, eram utilizados pela inteligência alemã e faziam parte do programa de armamento maciço de Hitler. Durante a Segunda Guerra Mundial, estima-se que mais de cem mil máquinas tenham sido produzidas. (SINGH, 2001)

Figura 15 – A máquina Enigma

Fonte: blogs.ne10.uol.com.br/mundobit/2015/01/21/como.fucionava-enigma-maquina-nazista-que-quase-venceu-segunda-guerra/

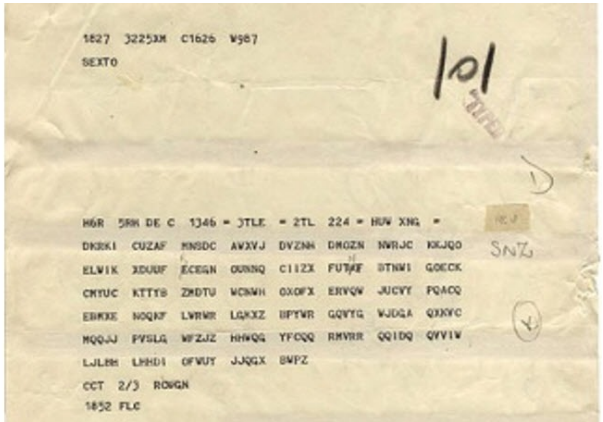
Calculando a quantidade possível de cifras do modelo antigo:

- Posições dos três rotores: $26 \times 26 \times 26 = 26^3 = 17.576$
- Sequência dos três rotores: $3! = 3 \times 2 \times 1 = 6$
- Substituir 6 pares de letras entre 26: $\dfrac{26!}{2^6 \times 6! \times 14!} = 100.391.791.500$

Total: $17.576 \times 6 \times 100.391.791.500 = 10.586.916.764.424.000$

Analisando uma combinação por minuto, levaria aproximadamente 20000000000 anos para realizar todas as tentativas.

Figura 16 – Mensagem criptografada pela Enigma



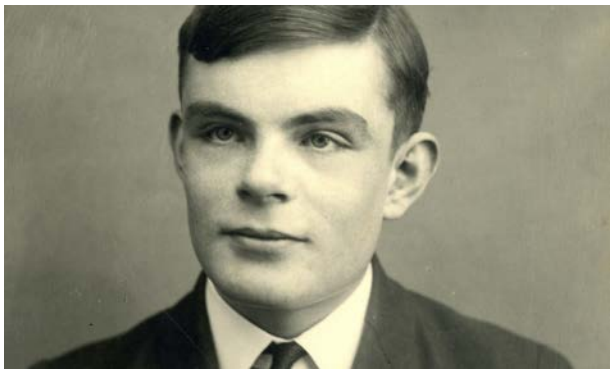
Fonte: pridecommerce.blogspot.com.br/2013/04/conheca-historia-da-criptografia

O sucesso da Enigma foi devido ao grande número de cifragens que poderiam ser utilizadas, fazendo com que fosse humanamente impossível decifrar as mensagens. Veja na figura 16 um exemplo de uma mensagem cifrada pela máquina Enigma. Observe, do lado direito da mensagem, três caracteres escritos a lápis que seriam a chave escolhida.

Segundo (SINGH, 2001), "se a necessidade é a mãe da invenção, então a adversidade talvez seja a mãe da criptoanálise".

Após muitas tentativas inúteis de decifrar a Enigma, um matemático brilhante chamado Alan Turing, obcecado pela ideia de produzir máquinas capazes de processar operações matemáticas, foi o escolhido para esse desafio. Em 1940, Alan Turing (Figura 17) e sua equipe da inteligência britânica construíram o primeiro computador operacional, ao qual apelidaram de Agnes, e seu propósito especificamente era decifrar mensagens alemãs cifradas pela máquina Enigma (SINGH, 2001). Com base nessa parte da história foi lançado, em 2014, o filme "O jogo da imitação". Aclamado pela crítica, foi indicado ao Oscar de melhor filme em 2015.

Figura 17 – Alan Turing



Fonte: www.huffingtonpost.es/2013/12/24/alang-turing-indultado_n_4497253.html

Muitas outras máquinas cifrantes e decifrantes foram inventadas, cada vez mais eficientes e rápidas. Colossus, por exemplo, inventada pelos britânicos em 1943 para decifrar a cifra alemã Lorenz, foi a primeira máquina programável. Foi essa característica que fez de Colossus o precursor do moderno computador digital.

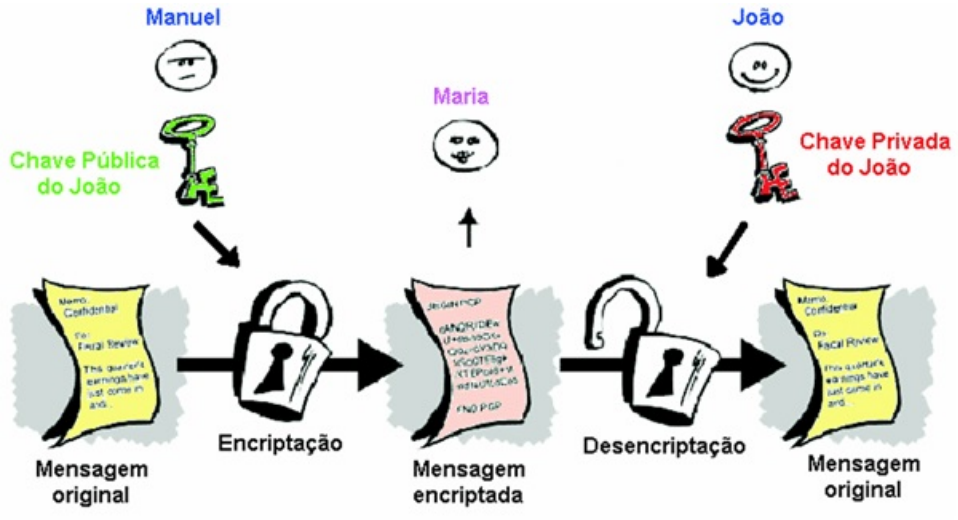
O avanço tecnológico nas décadas seguintes trouxe a necessidade de cifras cada vez mais complexas. Na década de 60 os computadores se tornaram mais poderosos e, ao mesmo tempo, mais baratos. Cada vez mais empresas eram capazes de comprar e manter computadores podendo utilizá-los também para cifrar comunicações importantes. Essa situação trouxe aos criptógrafos uma preocupação que não havia na época que a criptografia era um privilégio do governo e dos militares - a questão da padronização. Para que a troca de informação entre as empresas acontecesse de forma segura era necessária a criação de uma cifragem padrão.

Um dos algoritmos de cifragem mais usados, e candidato a padrão na época, era um

produto da IBM que foi desenvolvido na década de 70 por Horst Feistel, chamado Lucifer. Uma versão da cifra Lucifer foi oficialmente adotada em 1976 e batizada como Padrão de Cifragem de Dados (DES–Data Encryption Standart) e que, vinte cinco anos depois, continua sendo o padrão oficial americano para cifragem. (SINGH, 2001)

Mas ainda havia um sério problema a ser resolvido - a combinação e a distribuição das chaves. Motivados por esse problema é que os cientistas Whitfield Diffie e Martin Hellman, desenvolveram o conceito de criptografia de chave pública, sem dúvida um marco na história da criptografia. Na criptografia de chave pública (Figura 18) usam-se duas chaves distintas: uma chave chamada de pública e outra chave chamada de secreta (ou privada). A chave pública é usada para cifrar a mensagem enquanto a chave secreta é usada para decifrar a mensagem. (LOUREIRO, 2014)

Figura 18 – Esquema da criptografia de chave pública



Fonte: http://www.umsl.edu/ siegelj/information_theory/

A chave pública tem por finalidade:

- 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 que outra pessoa leia e altere a informação.

Já a chave privada é usada para decifrar a mensagem, sendo de conhecimento apenas do receptor da mensagem.

O mais interessante é que a chave pública não precisa ser mantida em segredo, por isso é pública. A única que precisa ser mantida em segredo é a chave privada. Assim

por exemplo, digamos que Maria queira enviar uma mensagem C para João. Então Maria consulta João para saber qual é a sua chave pública. Essa consulta não precisa ser feita em segredo, não tem problema se ela for interceptada por Manuel. João então responde que a chave pública é Ka. De posse da chave pública de João, Maria cifra a mensagem obtendo Ka(C) e envia para João. João então usando a chave privada Pa decifra a mensagem Pa(Ka(C)) = C. A chave pública e a privada são operações inversas, mas é importante ressaltar que a chave pública é construída de modo que não se pode determinar a chave privada a partir dela. (LOUREIRO, 2014)

Desse modo, Diffie e Hilman conseguiram brilhantemente idealizar a resolução do problema da distribuição de chaves mas não tinham nenhum exemplo de uma cifra de chave pública desenvolvido. A primeira cifra de chave pública apareceria um ano depois, em 1977, no MIT (Massachusetts Institute of Technology), com a equipe Ron Rivest, Adi Shamir e Len Adleman (Figura 19).

Figura 19 – Ron Rivest, Adi Shamir e Len Adleman

Fonte: http://www.umsl.edu/ siegelj/information_theory/

Esse sistema foi chamado de algoritmo assimétrico ou cifra assimétrica. A importância deste tipo de sistema é que viabiliza a troca de informações, de forma segura, via internet, sem haver a necessidade de combinar antecipadamente a chave entre emissor e receptor. Essa criptografia ficou conhecida como sistema RSA, cujas letras fazem referência aos nomes de seus criadores. (LOUREIRO, 2014)

Capítulo 2

Aprendendo sobre aprendizagem

Este capítulo tem o objetivo de esclarecer o processo de ensino e aprendizagem da Matemática por meio do estudo das principais teorias de aprendizagem. Consideramos de extrema importância dedicar uma parte deste trabalho para abordar tais teorias que tanto nos ajudaram na preparação das atividades propostas no quarto capítulo.

A Educação é um organismo vivo, ligado à formação do ser humano, que por sua vez está em constante mudança. É lógico que, por conta dessas mudanças do ser humano, muitas teorias, conjecturas, ideias e conhecimentos se formaram e ainda irão se formar.

> Não haveria educação se o homem fosse um ser acabado. O homem pergunta-se: Quem sou? De onde venho? Onde posso estar? O homem pode refletir sobre si mesmo e colocar-se num determinado momento, numa certa realidade: é um ser na busca constante de ser mais e, como pode fazer esta autorreflexão, pode descobrir-se como um ser inacabado, que está em constante busca. Eis aqui a raiz da educação. (FREIRE, 1979, p.12)

2.1 Influências de Piaget, Freire e Vygotsky

> Quando você observa seus alunos e avalia quanto cada um já sabe antes de introduzir um novo conceito em sala de aula está colocando em prática, mesmo sem se dar conta, as ideias de vários pesquisadores. Muitas atitudes que parecem apenas bom senso foram, ao longo dos anos, objeto de estudo de gente como Emilia Ferreiro, Célestin Freinet, Paulo Freire, Howard Gardner, Jean Piaget e Lev Vygotsky. Apesar de seus trabalhos não coincidirem em muitos aspectos, em outros tantos eles se complementam. (PELLEGRINI, 2001)

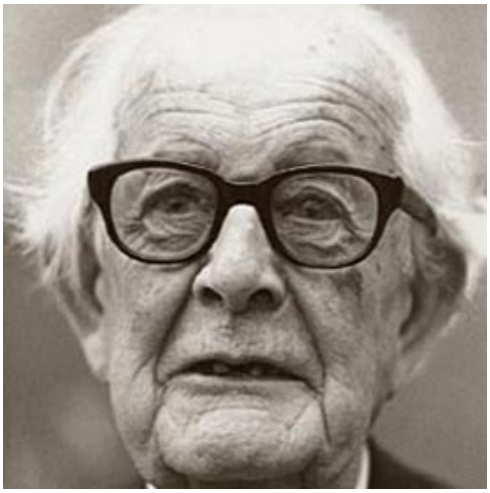
Todos os professores já estudaram em suas graduações conteúdos ligados a área da Educação como didática, pedagogia, psicologia, metodologia, dialética, aprendizagem, avaliação, entre outros vários tópicos que são de suma importância para nossa formação

profissional, mas o ser humano muda e com isso o processo educacional também sofre alterações.

> Tantos professores estão interessados nos aspectos teóricos da profissão por vários motivos. Em primeiro lugar, por sua atualidade. Todas essas ideias estão reunidas nos PCN. Além disso, já se foi o tempo em que uma corrente de pensamento era eleita a preferida (tal qual moda), enquanto as demais eram simplesmente esquecidas. (PELLEGRINI, 2001)

No que diz respeito a aprendizagem, muitas foram as contribuições desses pensadores ao longo dos últimos anos. Piaget, Freire e Vygotsky transformaram a educação, conquistaram e ainda conquistam uma série de seguidores/pesquisadores que, com base em suas ideias continuam a transformar o pensar e o agir de muitos profissionais da educação.

Figura 20 – Jean Piaget



Fonte: http://revistaescola.abril.com.br/pensadores/

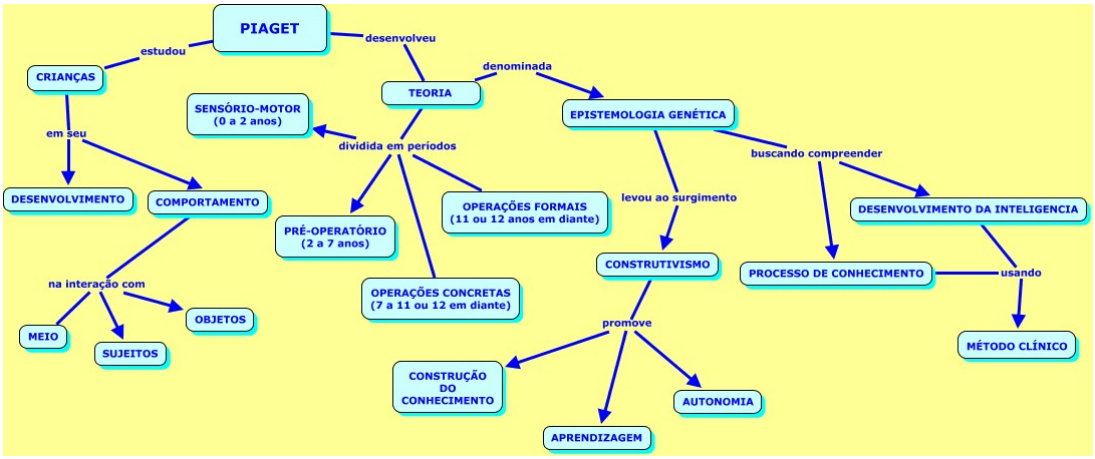
A teoria do desenvolvimento da inteligência foi desenvolvida pelo biólogo, psicólogo e epistemólogo suíço Jean Piaget (1896-1980) (Figura 20), que com base em suas experiências com crianças em várias faixas de idade, concluiu que o conhecimento não é somente fruto do meio que vive e nem é totalmente pertinente ao próprio sujeito, como as teorias da época baseavam-se.

Para Piaget, o conhecimento é construído através da relação do sujeito com seu meio, respeitando as suas estruturas cognitivas que dependem da sua maturidade. Os critérios de Piaget sobre educação levam em consideração o desenvolvimento da Psicologia, Biologia, Medicina, Filosofia e Antropologia. Diante disso o professor deve promover situações que induzam os alunos a encontrarem soluções práticas e corretas, de acordo com os níveis identificados. Essas ideias revolucionaram a educação e foram muito úteis para que houvesse um novo olhar para o aluno.

Na teoria piagetiana, a aprendizagem só ocorre quando as estruturas do pensamento se fixam e da mesma forma acontece com a passagem de um estágio para o outro do conhecimento, dependeria da fixação e superação do anterior ao qual está baseado. Em outras palavras, a criança só seria capaz de aprender o que sua mente é capaz de absorver de acordo com o seu desenvolvimento biológico (FERRARI, 2008). Era necessário haver um "desequilíbrio" daquilo que já é conhecido, um novo desafio, algo que colocasse as estruturas mentais em certa desordem para que a mente pudesse se reorganizar e dessa forma estabelecer um novo conhecimento. Isso deveria ser provocado no aluno pelo seu professor, o principal mediador do conhecimento.

Na figura 21 temos um mapa conceitual que ilustra muito bem a teoria piagetiana:

Figura 21 – Mapa conceitual da Teoria de Piaget



Fonte: http://metodologia43.pbworks.com/w/page/20815349/TEORIADEJEANPIAGET

Embora a teoria de Piaget tenha sido muito importante e inovadora, existem pontos que causaram certos conflitos com outros estudiosos do assunto. O fato de o desenvolvimento biológico superar o cognitivo foi muito questionado. Piaget também afirmava que crianças não eram capazes de pensar filosoficamente, que pensar sobre o pensar era algo impossível para uma criança. Muitos pesquisadores hoje afirmam o contrário, que é possível e que no mundo de hoje existem exemplos disso. (FERRARI, 2008)

De acordo com a teoria de Piaget, a Matemática deve ser utilizada como um instrumento capaz de promover a interpretação dos acontecimentos que estão ao nosso redor e no mundo, contribuindo na formação de pessoas com pensamento crítico, despertando na criança a capacidade de agir e refletir sobre o que aprende, respeitando as particularidades individuais do aluno, de forma que todos caminhem no mesmo sentido rumo ao aprendizado. (NOE, 2015)

A sala de aula de matemática deve criar condições para que a aprendizagem seja um processo ativo de elaboração, com o aluno construindo seu conhecimento. Então, se o professor de matemática, ao planejar sua aula, procurar motivar o aluno, desafiá-lo intelectualmente, quando leva em consideração sua maturação biológica, o impacto sofrido

por suas experiências de vidas, as trocas interpessoais aluno/professor – aluno/aluno e as transmissões culturais baseadas no meio em que vive, ele está pondo em prática as ideias construtivistas de Piaget. Aqui, o professor não é o detentor do saber mas o orientador, aquele que apresenta as questões. As estratégias de resolução de problemas, o uso de jogos, a modelagem matemática e mesmo a utilização de novas tecnologias, adaptam-se muito bem aos pressupostos piagetianos.

Lev Vygotsky (1896-1934), foi o responsável pela teoria chamada de sociointeracionista ou sociocultural, que recebe esse nome pela ênfase dada ao aspecto social. Os estudos de Vygotsky (Figura 22) sobre aprendizagem decorrem da compreensão do sujeito como um ser que se forma em contato com a sociedade, ou seja, somente através de uma dialética (debate), do sujeito com o outro e/ou com o meio, haverá um verdadeiro desenvolvimento sócio cognitivo.

Figura 22 – Lev Vygotsky

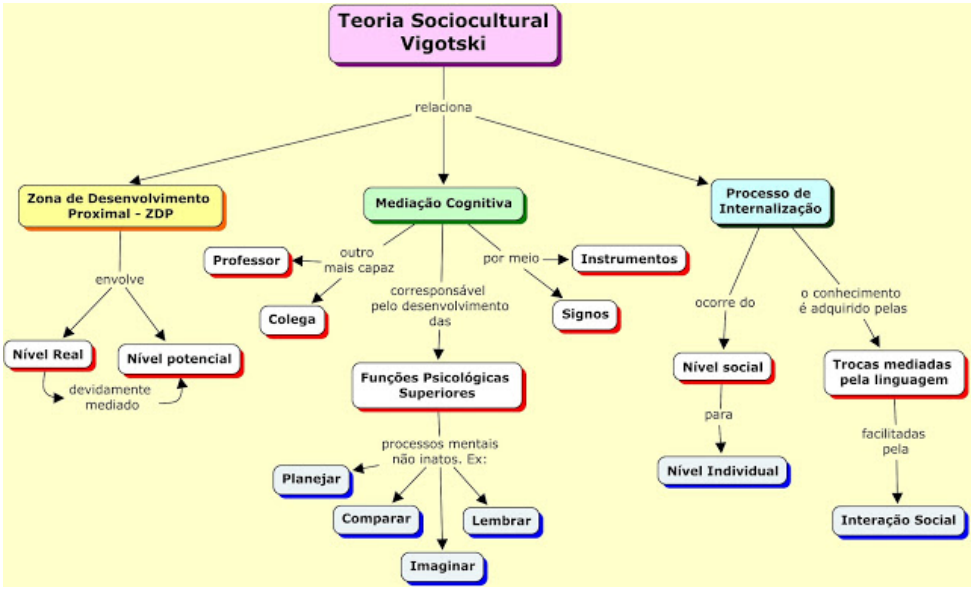
Fonte: http://revistaescola.abril.com.br/pensadores/

Vygotsky e seus colaboradores acreditavam estar correta a estrutura dos estágios cognitivos de Piaget, mas diferem quanto à evolução do processo. Enquanto Piaget defende que a aprendizagem só acontece após a maturidade das estruturas mentais superiores, priorizando o biológico ao social, para Vygotsky é o próprio processo de aprendizagem que gera e promove o desenvolvimento das estruturas mentais superiores, ou seja, um se desenvolve junto com o outro, portanto, quanto mais aprendizado, mais desenvolvimento.

(PAGANOTTI, 2011)

Na figura 23 temos um mapa conceitual ilustrando a teoria sociocultural de Vygotsky:

Figura 23 – Mapa conceitual da Teoria de Lev Vygotsky



Fonte:
http://psicologiadaeducacao-portfolio.blogspot.com.br/2013/02/mapa-conceitual-da-teoria-de-vigotsky.html

Sob a perspectiva da teoria sociocultural de Vygotsky, o ensino de matemática deve, primordialmente, mostrar a relação direta do que se está estudando com a realidade de vida do aluno, evitando que o saber matemático continue aparentando estar na contramão do saber da vida.

Sendo assim, quando um professor de matemática:

- valoriza em sala de aula a interação social, seja através de estudos em grupo, da contextualização de questões matemáticas ou de debates em salas de aula;
- busca diversas formas de explicar um conteúdo, seja oralmente, lendo e interpretando o enunciado, dando exemplos, fazendo esquemas ou usando novas tecnologias;
- elabora uma aula com níveis crescentes de abstração e generalização, partindo do familiar para o desconhecido, valorizando dessa forma o conhecimento prévio do aluno, ajudando-o durante o processo de aprendizagem, ou seja, intervindo no que Vygotsky chama de ZDP (Zona de Desenvolvimento Proximal), atualmente ZDI[1].

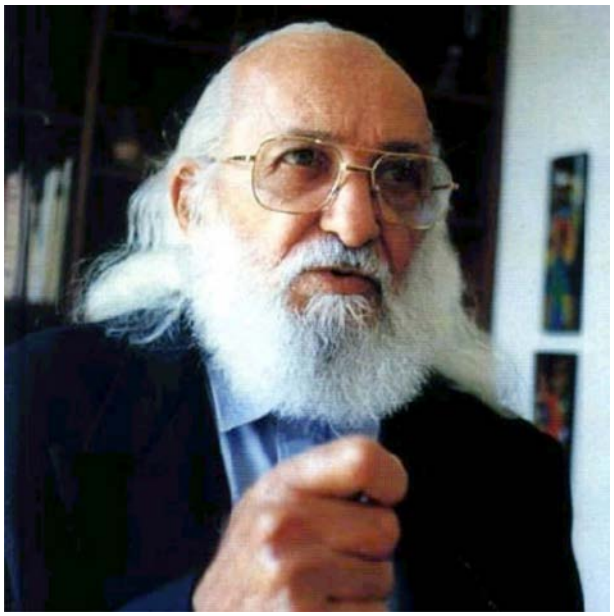
Ele está aplicando em suas aulas conceitos da Teoria Sociocultural de Vygotsky.

[1] Zona de Desenvolvimento Iminente - É a distância entre as práticas que uma criança já domina e as atividades nas quais ela ainda depende de ajuda. Para Vygotsky, é no caminho entre esses dois pontos que ela pode se desenvolver mentalmente por meio da interação e da troca de experiências. Não basta, portanto, determinar o que um aluno já aprendeu para avaliar seu desempenho.

Paulo Freire (1921-1997) foi um educador, pedagogista e filósofo muito influente no Brasil e no mundo. Autor de A Pedagogia do Oprimido, desenvolveu um pensamento pedagógico assumidamente político. Delineou uma Pedagogia da Libertação, intimamente relacionada com a visão marxista das consideradas classes oprimidas na tentativa de esclarecê-las e conscientizá-las politicamente. As suas maiores contribuições foram no campo da educação popular para a alfabetização e a conscientização política de jovens e adultos operários, chegando a influenciar em vários tipos de movimentos. Defendia que o objetivo da escola é ensinar o aluno a entender o mundo em que vive e assim poder transformá-lo. (FERRARI, 2008)

> Eu sou um intelectual que não tem medo de ser amoroso. Amo as gentes e amo o mundo. E é porque amo as pessoas e amo o mundo que eu brigo para que a justiça social se implante antes da caridade. (FREIRE, 1988)

Figura 24 – Paulo Freire



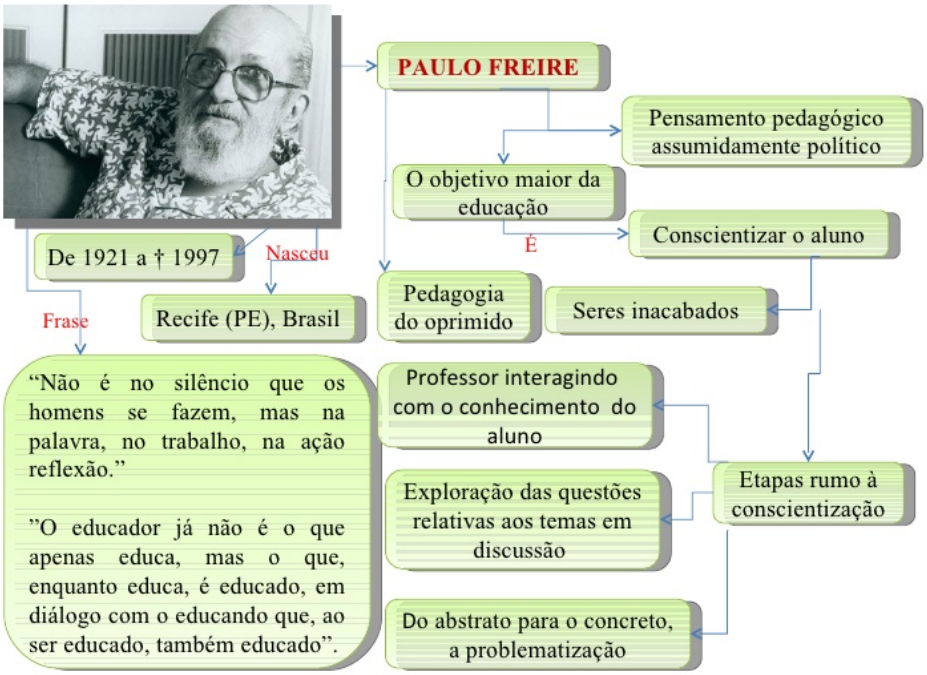
Fonte: https://localizarpaulofreirecies.blogspot.com.br/2016/02/paulo-freire.html

De acordo com Paulo Freire (Figura 24), a educação deve ser:

- **Libertadora** porque pode servir de importante instrumento de emancipação do homem diante da opressão;
- **Conscientizadora** porque promove o desenvolvimento crítico na tomada de consciência;
- **Autônoma** porque procura transformar o aluno em sujeito, o que implica na promoção da autonomia.

Segundo Paulo Freire, “Ensinar não é transferir conhecimento, mas criar as possibilidades para a sua produção ou a sua construção” (FREIRE, 1996, p.21). O professor deve transmitir o conhecimento buscando proporcionar ao aluno a compreensão do que foi exposto e, a partir daí, permitir que o mesmo dê um novo sentido ao conhecimento. A ideia é não dar respostas prontas, mas criar possibilidades, abrir oportunidades de indagações e sugestões, de raciocínio, de opiniões diversas etc. Jamais impedir as interações, as opiniões, os erros e os acertos, isto é, todos esses elementos permitirão que o aluno alcance o real conhecimento e continue a buscá-lo incessantemente de forma autônoma e prazerosa.

Figura 25 – Mapa conceitual da Teoria de Paulo Freire



Fonte: http://pt.slideshare.net/GraaSantos3/mapa-conceitual-gracasantos

A preocupação de tornar o educando um sujeito crítico, consciente da sua importância na sociedade e com condições de transformar sua vida, é parte do pensamento pedagógico político de Paulo Freire (Figura 25). O professor precisa explorar as questões relativas aos temas em discussão, isso permite que o aluno construa o caminho do senso comum para uma visão crítica da realidade. Ele deve ter a preocupação de sair do abstrato para o concreto, problematizar, criar situações, fazer com que o aluno busque, através de ações, soluções para as questões propostas. Paulo Freire considerava esses procedimentos como o caminho para objetivo final do ensino, que é a conscientização do aluno. (FERRARI, 2008)

Para Freire, o educador deve se inteirar daquilo que o aluno conhece, não apenas para poder avançar no ensino de conteúdos mas principalmente para trazer a cultura do aluno para dentro da sala de aula. De acordo com a teoria Freireana, o professor

de matemática precisa tornar esta ciência mais simples para o aluno. Isso não significa excluir sua profundidade e seu rigor, mas tornar simples a compreensão da matemática na existência humana. Sendo assim, é certo que o aluno terá a percepção da compreensão matemática.

2.2 Inteligências Múltiplas

A teoria das inteligências múltiplas foi desenvolvida pelo norte-americano Howard Gardner (Figura 26) e causou um grande impacto na área educacional quando foi divulgada no início da década de 1980.

Figura 26 – Howard Gardner

Fonte: https://www.gse.harvard.edu/faculty/howard-gardner

Gardner tem formação na área da psicologia e da neurologia, é professor de Cognição e Educação na Universidade de Harvard e professor de Neurologia na Universidade de Boston. Interessou-se pelos processos de aprendizagem nos primeiros estudos de pós-graduação quando pesquisou as descobertas de Piaget mas foi a sua experiência pessoal com a música e as artes, que começou na infância, que o levou a considerar o fato de haver múltiplas inteligências humanas. Naquela época, os testes de QI, criados nos primeiros anos do século 20 pelo psicólogo francês Alfred Binet, era o padrão mais aceito para a avaliação de inteligência. Esses testes mediam basicamente o raciocínio lógico-matemático e Gardner considerava que uma pessoa ter sua inteligência avaliada apenas através de uma única aptidão era totalmente parcial e insuficiente. (FERRARI, 2008)

Para Gardner, cada sociedade ou cultura é caracterizada por uma natureza cognitiva própria, com formas de expressão específicas em nível de pensamento. Na sociedade

americana, por exemplo, existe preconceitos sobre o que se entende por inteligência, que influenciam de forma negativa as escolas regulares:

- Westismo: palavra que se origina do inglês "West", que significa oeste. Fala da tendência em valorizar as habilidades linguísticas e matemáticas do indivíduo menosprezando outras habilidades. No Brasil também podemos ver claramente essa tendência, basta acompanharmos uma reunião de conselho de classe. Nelas os professores de Língua Portuguesa e Matemática são considerados os mais importantes e os melhores alunos são aqueles cujas maiores notas são nessas disciplinas.
- Bestismo: palavra que se originou na expressão inglesa "The best", que significa "O melhor". Onde se considera que o mais importante é ser sempre o melhor. As atividades escolares e a ação dos professores procuram igualar os alunos, ignorando suas diferenças individuais, padronizando as avaliações, de forma a destacar "os melhores" como aqueles que se destacam apenas nas áreas lingüísticas e lógico-matemáticas.
- Testismo: palava que se originou da palavra "Test". O Testismo está diretamente associado aos processos de avaliação nas escolas e envolve a suposição de que tudo que importa e tem valor, em termos de conhecimento, pode ser avaliado e mensurado através de testes e notas.

Atualmente, na teoria das inteligências múltiplas, Howard Gardner considera que a inteligência é composta por um espectro de oito competências, todas com a mesma dimensão e importância: linguística, lógico-matemática, interpessoal, intrapessoal, musical, espacial, corporal e naturalista. Gardner discutiu a possibilidade da existência de mais duas, a Espiritual e a Existencialista. No Brasil, alguns pesquisadores estão propondo a inclusão da competência pictórica. Vamos entender então um pouco mais a respeito dessas competências que compõem a inteligência humana e algumas profissões relacionadas (NOGUEIRA, 2007):

- Lingüística: criatividade com a palavra, perícia em lidar com idiomas, sensibilidade aos sons, estrutura, significados e funções das palavras - orador, escritor, poeta, jornalista, apresentador e advogado.
- Lógico-matemática: raciocínio dedutivo, perícia em resolver problemas, números, abstração de regras, estabelecer conjecturas, relações causais, etc - matemáticos, contadores, advogados, investigadores, cientistas e analistas de sistemas.
- Espacial: perícia de lidar com o espaço, de perceber o mundo viso espacial, de realizar transformações nas próprias percepções iniciais - arquiteto, navegador, pilotos, escultor.

- Corporal: capacidade de lidar com os movimentos do próprio corpo e de manejar objetos - artista, atleta, bailarinos, mágicos, malabaristas.
- Musical: capacidade de produzir e apreciar ritmo, tom e timbre; apreciação das formas de expressividade musical. Esta competência existe em estado puro, não relacionada a nenhuma outra – músico, cantor.
- Interpessoal: capacidade de relacionar-se bem com os outros, perícia em discernir e responder adequadamente aos estados de humor, temperamentos, motivações e desejos das outras pessoas - políticos, religiosos, líderes, psicólogos, "professores", "pais".
- Intrapessoal: é a competência que se refere ao "estar bem consigo mesmo", de discriminar as próprias emoções.
- Naturalista: capacidade de lidar com as várias espécies do meio ambiente - ecologistas e biólogos.

> A escola deve estimular a emergência dessas áreas, alimentando os interesses despertados, oferecendo canais adequados para sua manifestação e desenvolvimento. Não deve esquecer as áreas em que a criança se apresenta menos promissora, pois é fundamental estimular um desenvolvimento harmonioso do amplo espectro de competências. (NOGUEIRA, 2007)

De acordo com Gardner, são raríssimos os casos em que uma pessoa possui diversas inteligências desenvolvidas e são também raros os casos em que uma pessoa não possui nenhuma inteligência. Gardner ainda afirma que estas inteligências apresentam-se de duas formas. Algumas pessoas já nascem com determinadas inteligências, ou seja, a genética contribui. Porém, as experiências vividas também contribuem para o desenvolvimento de determinadas inteligências. O desenvolvimento mais ou menos apurado dessas competências depende de uma organização educacional que ajude a criança a atingir seu potencial máximo em cada uma delas. Para isso, é necessária uma variedade de disciplinas e atividades, todas de igual importância. Sob essa perspectiva, precisamos então estimular nossas crianças. Os pais precisam estar atentos às capacidades de seus filhos, nós professores devemos ter um olhar amplo em relação as possíveis capacidades de nossos alunos e a escola, por sua vez, deve oferecer a oportunidade do aluno ser capaz de desenvolver suas possíveis habilidades.

2.3 Aprendizagem significativa

Na década de 60, David Paul Ausubel (1918-2008), psicólogo e pesquisador norte-americano, formulou a teoria da aprendizagem significativa. Ausubel (Figura 27) baseou-se na premissa de que existe uma estrutura na qual organização e integração de aprendizagem

se processam. Para ele, o fator que mais influencia a aprendizagem é aquilo que o aluno já sabe ou o que pode funcionar como ponto de ancoragem para as novas ideias. (FERNADES, 2012)

Figura 27 – David Ausubel

Fonte: http://revistaescola.abril.com.br/img/210x210/david-ausubel.jpg

A aprendizagem significativa, conceito central da teoria de Ausubel, propõe-se a explicar o processo de assimilação que ocorre com a criança na construção do conhecimento a partir do seu conhecimento prévio, ou seja, envolve a interação de uma nova informação com uma estrutura de conhecimento que o aluno já possui, a qual define como conceito subsunçor. As informações no cérebro humano se organizam e formam uma hierarquia conceitual, na qual os elementos mais específicos de conhecimento são ligados e assimilados a conceitos mais gerais. O que contrapôs as ideias de Piaget, que não considera o progresso cognitivo consequência da soma de pequenas aprendizagens pontuais, mas sim um processo de equilibração desses conhecimentos. (BRUINI, 2015)

Dessa forma, para que ocorra uma aprendizagem significativa é necessário: disposição do sujeito para relacionar o conhecimento, material a ser assimilado com "potencial significativo" e existência de um conteúdo mínimo na estrutura cognitiva do indivíduo, com subsunçores em suficiência para suprir as necessidades relacionadas, no sentido cognitivo e afetivo. A assimilação de conhecimentos ocorre sempre que uma nova informação interage com outra existente na estrutura cognitiva, mas não com ela como um todo. O processo contínuo da aprendizagem significativa acontece apenas com a integração de conceitos relevantes. Segundo Ausubel, ensinar sem levar em conta a história de vida do aluno e o que ele já sabe é um esforço em vão, pois o novo conhecimento não tem onde se ancorar. (BRUINI, 2015)

É importante ressaltar que a teoria de Ausubel é uma teoria de aprendizagem em

sala de aula, pensada para o contexto escolar. Portanto, sua teoria fornece subsídios e favorece a compreensão das estratégias que o professor pode selecionar ou construir para efetivamente ensinar. No entanto, a responsabilidade pela aquisição de conhecimentos não depende apenas do professor. Ao contrário, depende muito do aluno. Enquanto o papel do professor é ser o facilitador do processo, o do aluno é decidir se quer aprender significativamente ou não. (BRUINI, 2015)

David Ausubel afirma que a aprendizagem significativa ocorre somente quando o aluno é capaz de perceber que os conhecimentos escolares são úteis para sua vida fora da escola. E, por isso, os professores precisam estar sempre atentos e refletirem sobre como ajudar os alunos a compreenderem a importância dos saberes escolares e a maneira de aplicá-los na vida em sociedade. (CERQUEIRA, 2013)

Duas estratégias desenvolvidas a partir das ideias de David Ausubel, e que são muito utilizadas atualmente para proporcionar uma aprendizagem significativa, são a sequência didática e o mapa conceitual.

As sequências didáticas são um conjunto de atividades concebidas e organizadas de tal forma que cada etapa está interligada à outra. Ao planejá-la, o professor tem como objetivo ensinar um determinado conteúdo, começando por uma atividade simples até chegar às operações mais complexas. Ou seja, elas são elaboradas de modo a respeitar os graus de dificuldade que os alunos irão encontrar nas tarefas, tornando possível sua superação. A sequência de atividades deve permitir a transformação gradual das capacidades iniciais dos alunos. As atividades podem ser concebidas com base no que os alunos já sabem e, a cada etapa, aumentar o grau de dificuldade, ampliando a capacidade desses estudantes. (CERQUEIRA, 2013)

Os mapas conceituais são estruturas que representam conjuntos de ideias e conceitos, dispostos em uma espécie de rede, de modo a apresentar mais claramente a exposição do conhecimento e organizá-lo segundo a compreensão cognitiva do seu idealizador. Indicam relações entre palavras e conceitos, desde aqueles mais abrangentes até os menos inclusivos. São utilizados para facilitar, ordenar e sequenciar os conteúdos a serem abordados, de modo a oferecer estímulos adequados à aprendizagem. Os mapas conceituais não são autoexplicativos, quem o faz é quem o explica. Os conceitos mais relevantes ficam nos retângulos. O conceito-chave deve aparecer em destaque. As linhas simbolizam as relações entre os conceitos. As palavras escritas sobre as linhas devem dar a ideia de proposições que expressam as relações entre os conceitos. (SILVA, 2012)

2.4 Conectivismo

Está em discussão o surgimento de uma nova teoria de aprendizagem chamada de Conectivismo. Essa nova teoria é defendida por George Siemens (Figura 28) e Stephen

Downes (Figura 29), pesquisadores na área de aprendizagem em rede, e seria uma teoria de aprendizagem para a era digital. Essa teoria é utilizada para explicar o efeito das novas tecnologias de informação e comunicação sobre a forma de como as pessoas vivem, se comunicam e aprendem.

Figura 28 – George Siemens

Fonte: http://ead.stj.jus.br/ead/pluginfile.php/17163/mod_resource/content/66/gsiemens_reg-res.jpg

Figura 29 – Stephen Downes

Fonte: http://octel.alt.ac.uk/wp-content/uploads/2013/04/Stephen-Downes.jpg

O Conectivismo se baseia na ideia de que o conhecimento existe no mundo, ao contrário do que pregam outras Teorias de Aprendizagem que afirmam que simplesmente existe na cabeça do indivíduo, ou seja, que a aprendizagem ocorre dentro da pessoa. Mesmo a visão construtivista social, que defende que a aprendizagem é um processo realizado socialmente, tem a pessoa como prioridade na aprendizagem. Estas teorias não abordam a aprendizagem que ocorre fora da pessoa, ou seja, a aprendizagem que é armazenada e manipulada através da tecnologia.

As teorias da aprendizagem estão preocupadas com o processo atual de aprendizagem, não com o valor do que está sendo aprendido. Em um mundo conectado, aquilo que buscamos aprender está diretamente ligado a sua importância. A necessidade de avaliar a importância de aprender alguma coisa é uma habilidade que é aplicada antes da própria aprendizagem começar. A capacidade de sintetizar e reconhecer conexões e padrões é algo muito valioso nos tempos atuais. Novas informações estão sendo continuamente adquiridas e a capacidade de reconhecer rapidamente quando novas informações vão alterar o que já foi feito é fundamental nesse nosso mundo de hoje. (SIEMENS, 2004)

Muitas questões importantes são levantadas quando as teorias de aprendizagem estabelecidas são vistas através da tecnologia. A tentativa natural dos teóricos é continuar a revisar e desenvolver as teorias na medida em que as condições mudam. Em algum ponto, no entanto, as modificações não são mais perceptíveis. É necessária uma abordagem inteiramente nova. (SIEMENS, 2004)

A inclusão da tecnologia e do fazer conexões, começam a mover as teorias de aprendizagem para uma idade digital. Não podemos mais, pessoalmente, experimentar e adquirir a aprendizagem de que necessitamos para agir. Nós alcançamos nossa competência como resultado da formação de conexões. A aprendizagem não está inteiramente sob o controle das pessoas, ela pode residir fora de nós mesmos. As conexões que nos capacitam a aprender são mais importantes que nosso estado atual de conhecimento. O conhecimento pessoal é composto por uma rede que alimenta as organizações e instituições, que por sua vez alimenta de volta a rede e então continua a prover aprendizagem para o indivíduo. Este ciclo de desenvolvimento do conhecimento permite que os aprendizes se mantenham atualizados em seus campos, através das conexões que formaram. (SIEMENS, 2004)

Segundo SIEMENS (2004), podemos resumir os princípios do Conectivismo nesses oito tópicos:

- Aprendizagem e conhecimento apoiam-se na diversidade de opiniões.
- Aprendizagem é um processo de conexão de informações.
- Aprendizagem pode residir em dispositivos não humanos.
- A capacidade de saber mais é mais crítica do que aquilo que é conhecido atualmente.
- É necessário cultivar e manter conexões para facilitar a aprendizagem contínua.
- A capacidade de enxergar conexões entre áreas, ideias e conceitos é uma habilidade fundamental.
- Atualização (“currency” – conhecimento acurado e em dia) é a intenção de todas as atividades de aprendizagem conectivistas.

- A tomada de decisão é, por si só, um processo de aprendizagem. Escolher o que aprender e o significado das informações que chegam é enxergar através das lentes de uma realidade em mudança. Apesar de haver uma resposta certa agora, ela pode ser errada amanhã devido a mudanças nas condições que cercam a informação e que afetam a decisão.

> O conectivismo apresenta um modelo de aprendizagem que reconhece as mudanças tectônicas na sociedade, onde a aprendizagem não é mais uma atividade interna, individualista. O modo como a pessoa trabalha e funciona são alterados quando se utilizam novas ferramentas. O campo da educação tem sido lento em reconhecer, tanto o impacto das novas ferramentas de aprendizagem como as mudanças ambientais na qual tem significado aprender. O conectivismo fornece uma percepção das habilidades e tarefas de aprendizagem necessárias para os aprendizes florescerem na era digital. (SIEMENS, 2004)

Capítulo 3

A Metodologia da Pesquisa

Pesquisar significa, de forma bem simples, procurar respostas para questões propostas. A pesquisa é um conjunto de ações, propostas para encontrar a solução para um problema, que têm por base procedimentos racionais e sistemáticos. É realizada quando se tem um problema e não se têm informações para solucioná-lo.

A investigação científica depende de um conjunto de procedimentos intelectuais e técnicos que se devem empregar na investigação para que os objetivos da pesquisa sejam atingidos. A esse conjunto de procedimentos e técnicas damos o nome de metodologia científica.

A pesquisa científica seria, portanto, a realização concreta de uma investigação planejada e desenvolvida de acordo com as normas consagradas pela metodologia científica.

Entendemos como metodologia científica um conjunto de etapas ordenadamente dispostas que você deve vencer na investigação de um fenômeno. Nessas etapas estão incluídos desde a escolha do tema, o planejamento da investigação, o desenvolvimento metodológico, a coleta de dados, a análise dos resultados, a elaboração das conclusões e até a divulgação de resultados.

Realizar uma pesquisa com rigor científico pressupõe que você escolha um tema e defina um problema para ser investigado, elabore um plano de trabalho e, após a execução operacional desse plano, escreva um relatório final e este seja apresentado de forma planejada, ordenada, lógica e conclusiva. (SILVA; MENEZES, 2005)

Nesse capítulo abordaremos os aspectos metodológicos que estruturaram esse trabalho.

3.1 Método Científico

O método científico que norteou essa pesquisa foi o fenomenológico. Esse método preocupa-se com a descrição direta da experiência tal como ela é. A realidade é construída

socialmente e entendida como o compreendido, o interpretado, o comunicado. Então, a realidade não é única: existem tantas quantas forem as suas interpretações e comunicações. O sujeito/ator é reconhecidamente importante no processo de construção do conhecimento. (SILVA; MENEZES, 2005)

A fenomenologia, tomada como uma postura frente à Educação, oportuniza ao professor focar o aluno, ou seja, compreender o modo de ser do aluno e o cuidado no que diz respeito à sua formação como ser humano. A fenomenologia procura olhar o fenômeno em sua totalidade, sem preconceitos ou um quadro teórico prévio, porém sabe que olhar na totalidade não é dar conta do todo, mas do perfil que aparece na síntese. É uma postura de interrogação. O fenômeno é olhado primeiramente como ele se apresenta no mundo, pelo pesquisador que o intenciona. (KLUBER; BURAK, 2008)

A Educação aqui não é entendida como um objeto, mas sim como um fenômeno. Tomando-se a Educação Matemática como fenômeno, e as possibilidades investigativas que se podem realizar no seu contexto, considera-se que a Fenomenologia pode contribuir significativamente, pois permite o desenvolvimento de uma pesquisa qualitativa que não é definida a priori, com resultados e hipóteses já esperados. Remete o investigador para uma visão de construção do conhecimento e da realidade. Por isso, não concebe, nem uma e nem outra, como prontas e acabadas. Essa abertura não permite a estagnação do conhecimento já produzido historicamente, porque procura dar-lhe significado, assim como à realidade que se constrói pelo sujeito. (KLUBER; BURAK, 2008)

No que concerne ao conteúdo matemático e às pesquisas que se voltam para o ensino e para a aprendizagem da Matemática, a postura fenomenológica pode favorecer a ruptura das formas predominantes de transmissão de conteúdos. Isso se torna possível a partir da compreensão de que a fenomenologia busca o significado, o sentido de o homem estar no mundo, do seu fazer, dos seus atos que são sempre intencionais. Educador e educandos buscam aquilo que faz sentido para eles na relação com o mundo. A Matemática tem novo significado e é compreendida como uma construção sócio-histórica, inclusive por diferentes culturas. Outros fatores, além do lógico, podem adentrar a sala de aula, para fortalecer o processo de ensino e de aprendizagem, como a emoção, a história, as relações culturais e outras. A liberdade de não ter que comprovar hipóteses, nem dar respostas apenas adequadas, no sentido de um pensar único, fechado ou "ideal", para a comprovação de uma teoria, confere uma outra forma de ver a pesquisa em Educação Matemática. (KLUBER; BURAK, 2008)

> Os procedimentos metodológicos da pesquisa qualitativa fenomenológica fazem sentido nas investigações em Educação Matemática, haja vista que, nos últimos anos, as investigações têm se voltado para a formação de professores, práticas docentes, capacidade de aprendizagem dos alunos, pesquisas etnográficas, pesquisas em Etnomatemática e Modelagem Matemática. Para dar conta das interpretações percebidas nessas investigações, a descrição, a interpretação por meio da hermenêutica e a explicitação dos

> resultados se mostram significativos. Os dados são muitos e as interpretações não ficam apenas no âmbito da linguagem, ou da quantificação, porque abarcam, como um todo, a experiência vivida pelo pesquisador e pelos demais sujeitos da pesquisa. Portanto, a Fenomenologia, do ponto de vista epistemológico, leva em consideração a história, a cultura, o social, o antropológico, enfim, a busca da totalidade da compreensão que o sujeito possui em determinado momento em que se encontra, em seu mundo-vida. (KLUBER; BURAK, 2008)

3.2 Classificação da Pesquisa

Do ponto de vista da sua natureza, essa pesquisa pode ser considerada aplicada pois objetiva gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos. Envolve verdades e interesses locais (PRODANOV; FREITAS, 2013). De fato, esse trabalho tem aplicação direta na sala de aula de Matemática no ensino fundamental. As atividades aqui propostas foram elaboradas com o objetivo de fornecer uma opção diferente de material de trabalho para o professor de matemática. Essas atividades abordam um tema com aplicações atuais, com uma linguagem mais acessível para o aluno e sem a necessidade de grandes conhecimentos matemáticos prévios. De acordo com as teorias de aprendizagem estudadas no segundo capítulo, essa estratégia de ensino contribui para estimular a aprendizagem da matemática.

Quanto aos objetivos, consideramos que seja uma pesquisa explicativa. Nesse tipo de pesquisa o pesquisador procura explicar os porquês das coisas e suas causas, por meio do registro, da análise, da classificação e da interpretação dos fenômenos observados. Visa a identificar os fatores que determinam ou contribuem para a ocorrência dos fenômenos, ou seja, dos problemas observados. (PRODANOV; FREITAS, 2013)

A criptografia é um tema ainda pouco explorado, não faz parte do conteúdo do currículo mínimo da educação básica e sua aplicabilidade matemática é pouco divulgada em livros didáticos. Observamos esse problema e consideramos que, tanto docentes quanto discentes, estão perdendo uma grande aliada para o ensino e aprendizagem da matemática.

Muitos professores de matemática tem dificuldade de produzir uma aprendizagem significativa no aluno. Esse fato está relacionado, em parte, a maneira com que a matemática é ensinada em sala de aula, de uma forma repetitiva, desgastante e distante da realidade do aluno. Isso impede que o discente entenda sua importância e aplicabilidade no seu cotidiano.

A Criptografia é um tema bastante atual e sua aplicação matemática é bem diversificada, possibilitando a utilização de vários conteúdos matemáticos do ensino fundamental. A introdução da criptografia em sala de aula não será de forma alguma trabalhosa, visto que não se faz necessário nenhum conhecimento prévio para seu entendimento. Utilizamos essas vantagens da criptografia para elaborar atividades que auxiliem o professor no seu

trabalho, incentivando os alunos a se encantarem pela matemática.

De acordo com a forma de abordagem do problema essa pesquisa se caracteriza como qualitativa. Na pesquisa qualitativa existe uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa. A pesquisa tem o ambiente como fonte direta para coleta dos dados e o pesquisador é o instrumento-chave mantendo contato direto com o ambiente e o objeto de estudo em questão, necessitando de um trabalho mais intensivo de campo. Nesse caso, as questões são estudadas no ambiente em que elas se apresentam sem qualquer manipulação intencional do pesquisador. (PRODANOV; FREITAS, 2013)

A utilização desse tipo de abordagem difere da abordagem quantitativa pelo fato de não utilizar dados estatísticos como o centro do processo de análise de um problema, não tendo, portanto, a prioridade de numerar ou medir unidades. Preocupa-se muito mais com o processo do que com o produto. Na análise dos dados coletados, não há preocupação em comprovar hipóteses previamente estabelecidas. (PRODANOV; FREITAS, 2013)

3.3 Procedimentos Técnicos

Quanto aos procedimentos técnicos, apresenta características da pesquisa de campo.

A pesquisa de campo é aquela utilizada com o objetivo de conseguir informações e/ou conhecimentos acerca de um problema para o qual procuramos uma resposta, ou de uma hipótese, que queiramos comprovar, ou, ainda, descobrir novos fenômenos ou as relações entre eles. Consiste na observação de fatos e fenômenos tal como ocorrem espontaneamente, na coleta de dados a eles referentes e no registro de variáveis que presumimos relevantes, para analisá-los. As fases da pesquisa de campo requerem, em primeiro lugar, a realização de uma pesquisa bibliográfica sobre o tema em questão. Ela servirá, como primeiro passo, para sabermos em que estado se encontra atualmente o problema, que trabalhos já foram realizados a respeito e quais são as opiniões reinantes sobre o assunto. Como segundo passo, permitirá que estabeleçamos um modelo teórico inicial de referência, da mesma forma que auxiliará na determinação das variáveis e na elaboração do plano geral da pesquisa. Em segundo lugar, de acordo com a natureza da pesquisa, determinamos as técnicas que serão empregadas na coleta de dados e na definição da amostra, que deverá ser representativa e suficiente para apoiar as conclusões. (SILVA; MENEZES, 2005)

A pesquisa bibliográfica se caracteriza por ser elaborada a partir de material já publicado, constituído principalmente de: livros, revistas, publicações em periódicos e artigos

científicos, jornais, boletins, monografias, dissertações, teses, material cartográfico, internet, com o objetivo de colocar o pesquisador em contato direto com todo material já escrito sobre o assunto da pesquisa. Em relação aos dados coletados na internet, devemos atentar à confiabilidade e fidelidade das fontes consultadas eletronicamente. (SILVA; MENEZES, 2005)

Nossa pesquisa bibliográfica foi composta por duas partes muito importantes para a elaboração das atividades propostas: a História da Criptografia e as Teorias de Aprendizagem. O contexto histórico foi fundamental para introduzir as atividades e explorar a interdisciplinaridade. O estudo das Teorias de Aprendizagem contribuiu para a estruturação didática das atividades.

Como já mencionado, utilizamos como modelo teórico inicial de referência a pesquisa do professor LOUREIRO (2014), complementando esse estudo por meio de atividades voltadas para o ensino fundamental.

3.4 Instrumento da pesquisa

3.4.1 Atividades

Consideramos que o estudo da criptografia em sala de aula venha a contribuir para uma intimidade maior do aluno com a matemática, possibilitando uma visão mais otimista do discente com respeito a esta ciência.

Assim, preparamos um material diferenciado para o professor, constituído de quatro atividades. Cada atividade aborda um tópico de criptografia, com uma linguagem simples e de fácil entendimento para professores e alunos, visando facilitar o trabalho do docente, estimular a aprendizagem da matemática e despertar o interesse do aluno pela mesma.

Ao elaborar as atividades utilizando a criptografia e as cifras simétricas, seguimos uma sequência didática. Aumentamos gradativamente o nível de dificuldade em cada atividade, introduzindo sempre um assunto novo baseando-se em outro já solidificado, levando sempre em consideração o conhecimento prévio do aluno, desenvolvendo assim seu raciocínio lógico e propiciando uma aprendizagem significativa. Fizemos conexões entre vários conteúdos matemáticos e a criptografia. Procuramos trabalhar a interdisciplinaridade com a disciplina de História, por meio da História da Criptografia, e com a disciplina de Língua Portuguesa, por meio da leitura, da interpretação de texto e do vocabulário.

Capítulo 4

A criptografia no Ensino Fundamental II

Neste capítulo, organizamos atividades a serem aplicadas a partir do sexto ano do ensino fundamental. Nelas buscamos fazer conexões entre criptografia, a aprendizagem da matemática e seus conteúdos. Pretendemos, com essas atividades, oferecer ao professor de Matemática um material diferente para ser utilizado em sala de aula, com o objetivo de estimular a aprendizagem e despertar o interesse do educando. A interdisciplinaridade também está presente e é um aspecto relevante. Fazer ligações entre a matemática e as outras disciplinas enriquece a aula e torna o conhecimento mais significativo.

A Criptografia não está no currículo mínimo do ensino fundamental mas pode ser utilizada como um conector entre os conteúdos matemáticos e o cotidiano do discente. A intenção é fazer com que o mesmo amplie seu conhecimento e constate a dimensão da Matemática, ao identificar sua presença constante no dia a dia.

4.1 Atividade 1 - Introdução à Criptografia

4.1.1 Objetivos da atividade

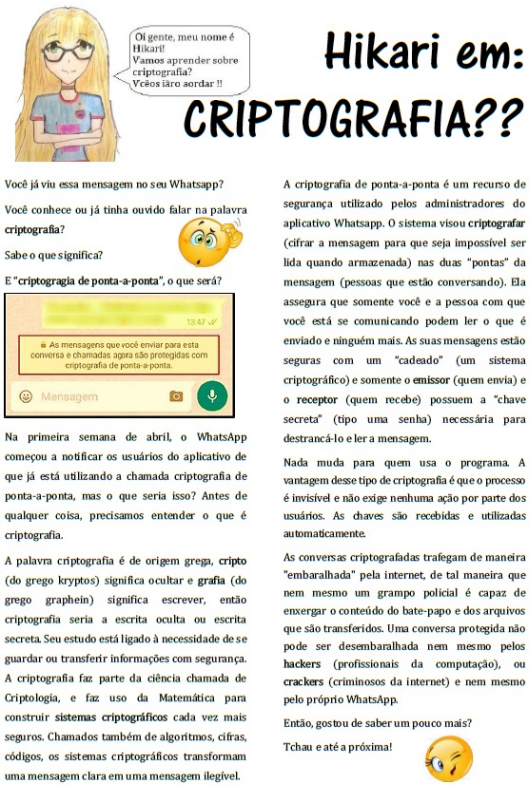
Essa primeira atividade terá a duração de aproximadamente 1h 40 minutos. O objetivo é introduzir e conceituar o tema Criptografia, despertando a curiosidade e o interesse dos alunos pelo tema.

As teorias de Piaget, Freire e Vygotsky compartilham a ideia de que o conhecimento é construído através da relação do sujeito com seu meio, em um processo ativo de elaboração, levando em consideração as experiências de vida do aluno, e as trocas interpessoais em sala de aula. Estruturamos essa atividade baseados nessas características. No texto, utilizamos o aplicativo Whatsapp - presente no dia a dia da maioria dos estudantes - para introduzir o estudo da Criptografia e também como tema da dinâmica. Nesta, os alunos serão motivados a pensar de forma crítica sobre a necessidade de proteger informações. Essa preocupação com o desenvolvimento do pensamento crítico é outro fator presente nas

teorias de aprendizagem estudadas no terceiro capítulo, principalmente na teoria Freiriana. Outra ideia presente nessa atividade é a de produzir no aluno a capacidade de fazer conexões. Segundo o Conectivismo de George Siemens, em um mundo conectado, a necessidade de avaliar a importância de aprender alguma coisa é uma habilidade que é aplicada antes da própria aprendizagem começar. Ao perceber a importância da aplicação Matemática na Criptografia ao longo da história e nos dias atuais, o aluno entende a necessidade deste estudo, e de fazer conexões entre a Matemática e a aplicação da mesma no seu dia a dia.

4.1.2 O material utilizado

Figura 30 – Texto da Atividade 1



Hikari em:
CRIPTOGRAFIA??

Você já viu essa mensagem no seu Whatsapp?

Você conhece ou já tinha ouvido falar na palavra **criptografia**?

Sabe o que significa?

E "**criptografia de ponta-a-ponta**", o que será?

Na primeira semana de abril, o WhatsApp começou a notificar os usuários do aplicativo de que já está utilizando a chamada criptografia de ponta-a-ponta, mas o que seria isso? Antes de qualquer coisa, precisamos entender o que é criptografia.

A palavra criptografia é de origem grega, **cripto** (do grego kryptos) significa ocultar e **grafia** (do grego graphein) significa escrever, então criptografia seria a escrita oculta ou escrita secreta. Seu estudo está ligado à necessidade de se guardar ou transferir informações com segurança. A criptografia faz parte da ciência chamada de Criptologia, e faz uso da Matemática para construir **sistemas criptográficos** cada vez mais seguros. Chamados também de algoritmos, cifras, códigos, os sistemas criptográficos transformam uma mensagem clara em uma mensagem ilegível.

A criptografia de ponta-a-ponta é um recurso de segurança utilizado pelos administradores do aplicativo Whatsapp. O sistema visou **criptografar** (cifrar a mensagem para que seja impossível ser lida quando armazenada) nas duas "pontas" da mensagem (pessoas que estão conversando). Ela assegura que somente você e a pessoa com que você está se comunicando podem ler o que é enviado e ninguém mais. As suas mensagens estão seguras com um "cadeado" (um sistema criptográfico) e somente o **emissor** (quem envia) e o **receptor** (quem recebe) possuem a "chave secreta" (tipo uma senha) necessária para destrancá-lo e ler a mensagem.

Nada muda para quem usa o programa. A vantagem desse tipo de criptografia é que o processo é invisível e não exige nenhuma ação por parte dos usuários. As chaves são recebidas e utilizadas automaticamente.

As conversas criptografadas trafegam de maneira "embaralhada" pela internet, de tal maneira que nem mesmo um grampo policial é capaz de enxergar o conteúdo do bate-papo e dos arquivos que são transferidos. Uma conversa protegida não pode ser desembaralhada nem mesmo pelos **hackers** (profissionais da computação), ou **crackers** (criminosos da internet) e nem mesmo pelo próprio WhatsApp.

Então, gostou de saber um pouco mais?

Tchau e até a próxima!

Fonte: Elaborado pela autora (vide anexo A)

Foi elaborado um texto pela autora desse trabalho, onde a personagem Hikari explica o que é Criptografia. O texto (Figura 30) utiliza uma mensagem que está no Aplicativo Whatsapp para introduzir o tema. A personagem faz questionamentos que despertam a curiosidade pela leitura do texto. É importante que o aluno perceba o quanto a Criptografia está presente nos dias de hoje, sua importância na vida das pessoas e o significado da Matemática nesse contexto.

4.1.3 Desenvolvimento da atividade

O professor deverá distribuir o texto e perguntar se alguém deseja ler e, se mais de um aluno desejar fazê-lo, permitir que cada um leia um pouco. Se não houver manifestação, cabe ao professor ler o texto. Com o auxílio do texto e das perguntas contidas o professor deverá verificar o conhecimento dos alunos a respeito do assunto. No texto, algumas palavras foram destacadas e o professor deverá se certificar de que seus significados foram esclarecidos e bem entendidos.

No segundo momento da atividade o professor aplicará uma dinâmica chamada Whatsapp de papel: trocas de mensagens entre os alunos. Para esta, o professor deverá distribuir um pedaço de papel para cada aluno, organizando-os em círculo, cada um escolherá um colega para a troca da mensagem mas a dupla não deverá estar próxima. Depois de formadas as duplas, cada aluno escreverá uma pequena mensagem de otimismo para o colega, assinando-a no final. O papel deverá ser dobrado ao meio e ao meio de novo, de forma que não se possa ler seu conteúdo. O nome do outro aluno que irá receber a mensagem deverá ser escrito por fora. As mensagens devem ser passadas de aluno por aluno pelo lado direito até chegarem ao seu destino. Nesse momento da dinâmica o professor deverá intervir, procurando interceptar as mensagens, lendo seu conteúdo ou incentivando os discentes que façam o mesmo com as mensagens dos colegas. Evidenciar que é fácil interceptar uma mensagem de alguém se esta não estiver bem protegida. E aí, ressaltar a necessidade da proteção das informações, sejam elas importantes ou não, pessoais ou de um grupo, de pessoas ou empresas, faz-se a cada dia mais necessário.

Então o professor deve concluir a dinâmica sugerindo que os alunos pensem em formas de criptografar suas mensagens, dando-lhes dicas e ouvindo suas ideias.

4.1.4 Concluindo a atividade

Nessa atividade, haverá o primeiro contato com a Criptografia, sua utilização e importância para a vida das pessoas. Após, os alunos estarão aptos a irem mais adiante e prontos para a atividade 2. Antes de iniciar a próxima atividade, conferir se conseguiram criptografar suas mensagens. Sinalizar a importância de manter em segredo o sistema criptográfico criado e pedir que seja anotado e guardado para não se esquecer.

4.2 Atividade 2 - Cifra Simétrica de Transposição

4.2.1 Objetivos da atividade

Dar os primeiros passos na Criptografia. Aprender sobre o método de cifragem por transposição, levá-lo-á ao conhecimento de uma parte da sua História, e assim, começará a

cifrar e decifrar pequenas mensagens utilizando a cifra simétrica de transposição. Deverá ter a duração de no máximo dois tempos de aula (1h e 40 minutos).

Nessa etapa, o aluno já possui a base necessária para avançarmos um pouco mais. Segundo David Ausubel, na teoria da aprendizagem significativa, o fator que mais influencia a aprendizagem é aquilo que o aluno já sabe ou o que pode funcionar como ponto de ancoragem para as novas ideias. Na teoria sociocultural, Vygotsky também acredita que valorizar o conhecimento prévio do aluno, partindo do familiar para o desconhecido, e com níveis crescentes de abstração, facilita a aprendizagem e torna o conhecimento mais significativo.

Ao aplicar a atividade, exploraremos montagem de tabelas de acordo com número de linhas e colunas, assim como transposição de colunas no processo de cifragem de mensagens. Estar familiarizado com estes assuntos matemáticos será de grande ajuda futura para nossos discentes, servindo de apoio para novos conteúdos.

4.2.2 Material utilizado

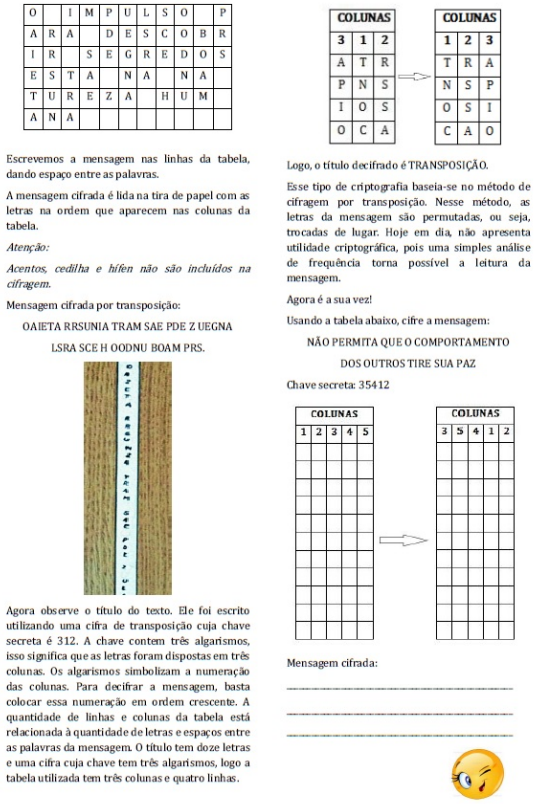
Figura 31 – Texto da Atividade 2

Fonte: Elaborado pela autora (vide anexo B)

Foi elaborado um texto pela autora (Figura 31), onde a personagem Hikari explica sobre o método de cifragem por transposição. Conta também a história sobre a Cítala, ou Bastão de Licurgo, utilizado pelos Espartanos, e ensina a construir uma cítala caseira. Para esta, precisaremos de lápis, uma tira de papel A4 de 1 cm de largura e caneta para escrever a mensagem.

Por fim, a personagem usa o título cifrado por transposição para exemplificar esse método de cifragem. É utilizado uma tabela montada a partir da chave secreta (Figura 32). Para aplicar o conhecimento adquirido no texto, o aluno fará um exercício de cifragem com uma chave de cinco algarismos.

Figura 32 – Continuação do Texto da Atividade 2



O		I	M	P	U	L	S	O		P
A	R	A		D	E	S	C	O	B	R
I	R		S	E	G	R	E	D	O	S
E	S	T	A		N	A		N	A	
T	U	R	E	Z	A		H	U	M	
A	N	A								

Escrevemos a mensagem nas linhas da tabela, dando espaço entre as palavras.

A mensagem cifrada é lida na tira de papel com as letras na ordem que aparecem nas colunas da tabela.

Atenção:

Acentos, cedilha e hífen não são incluídos na cifragem.

Mensagem cifrada por transposição:

OAIETA RRSUNIA TRAM SAE PDE Z UEGNA

LSRA SCE H OODNU BOAM PRS.

Agora observe o título do texto. Ele foi escrito utilizando uma cifra de transposição cuja chave secreta é 312. A chave contem três algarismos, isso significa que as letras foram dispostas em três colunas. Os algarismos simbolizam a numeração das colunas. Para decifrar a mensagem, basta colocar essa numeração em ordem crescente. A quantidade de linhas e colunas da tabela está relacionada à quantidade de letras e espaços entre as palavras da mensagem. O título tem doze letras e uma cifra cuja chave tem três algarismos, logo a tabela utilizada tem três colunas e quatro linhas.

COLUNAS		
3	1	2
A	T	R
P	N	S
I	O	S
O	C	A

COLUNAS		
1	2	3
T	R	A
N	S	P
O	S	I
C	A	O

Logo, o título decifrado é TRANSPOSIÇÃO.

Esse tipo de criptografia baseia-se no método de cifragem por transposição. Nesse método, as letras da mensagem são permutadas, ou seja, trocadas de lugar. Hoje em dia, não apresenta utilidade criptográfica, pois uma simples análise de frequência torna possível a leitura da mensagem.

Agora é a sua vez!

Usando a tabela abaixo, cifre a mensagem:

NÃO PERMITA QUE O COMPORTAMENTO

DOS OUTROS TIRE SUA PAZ

Chave secreta: 35412

COLUNAS				
1	2	3	4	5

COLUNAS				
3	5	4	1	2

Mensagem cifrada:

Fonte: Elaborado pela autora (vide anexo B)

4.2.3 Desenvolvimento da atividade

O professor deverá distribuir o texto e desenvolver a atividade juntamente com os alunos. O texto deverá ser lido e explicado até que nenhuma dúvida paire. Para a construção da Cítala o professor deverá pedir com antecedência a providência do material. São materiais comuns, fáceis de se conseguir e de baixo custo. Toda a construção estará explicada no texto, assim como a forma de cifragem.

O exercício foi baseado no exemplo dado no texto. O professor deverá esclarecer a lógica de montagem da tabela e formulação da chave. Antes de cifrar a mensagem, deve-se contar primeiro a quantidade de letras possuídas e os espaços entre as palavras. A tabela deverá conter uma quantidade de lacunas suficientes para as letras da mensagem. O discente deverá entender que o número de linhas (fileiras horizontais) multiplicado pelo número de colunas (fileiras verticais) terá como resultado a quantidade de lacunas da tabela.

Esta dependerá da quantidade de algarismos da chave. A mensagem deverá ser escrita, preenchendo linha por linha da tabela. Os algarismos da chave são a ordem das colunas. Colocando-os nas colunas de acordo com a ordem em que aparece na chave teremos a mensagem cifrada. Para decifrar, basta colocar as colunas dos algarismos das chaves em ordem crescente.

Resposta da atividade (Figura 33):

Mensagem: NÃO PERMITA QUE O COMPORTAMENTO DOS OUTROS TIRE SUA PAZ

Figura 33 – Colunas preenchidas

COLUNAS				
1	2	3	4	5
N	A	O		P
E	R	M	I	T
A		Q	U	E
	O		C	O
M	P	O	R	T
A	M	E	N	T
O		D	O	S
	O	U	T	R
O	S		T	I
R	E		S	U
A		P	A	Z

COLUNAS				
3	5	4	1	2
O	P		N	A
M	T	I	E	R
Q	E	U	A	
	O	C		O
O	T	R	M	P
E	T	N	A	M
D	S	O	O	
U	R	T		O
	I	T	O	S
	U	S	R	E
P	Z	A	A	

Fonte: Elaborado pela autora

Chave secreta: 35412

Mensagem cifrada: OP NAMTIERQEUA OC OOTRMPETNAMDSOO URT O ITOS USRE PZAA

4.2.4 Concluindo a atividade

Ao final da atividade, o aluno deverá ser capaz de cifrar ou decifrar uma mensagem cifrada por transposição utilizando a tabela e a chave.

4.3 Atividade 3 - Cifra Simétrica de Substituição Monoalfabética

4.3.1 Objetivos da atividade

Com duração de aproximadamente 1h e 40 minutos, tem como objetivo estimular o discente a aprendizagem de conteúdos matemáticos por meio do estudo da Criptografia. Assim, aprenderá um pouco mais sobre as características e classificações da Criptografia, conhecerá mais de sua História e começará a cifrar e decifrar pequenas mensagens utilizando a cifra simétrica de substituição monoalfabética. Nessa etapa, os conteúdos abordados serão: números naturais, números primos e múltiplos. Esses conteúdos serão ferramentas na formação de enigmas para descoberta da chave secreta.

Segundo Howard Gardner, devemos respeitar as habilidades de cada indivíduo. Valorizar apenas a inteligência lógico-matemática no discente, desprezando suas possíveis competências, exerce uma influência negativa em relação à Matemática. Ao introduzir assuntos diferentes, mais atuais, saindo do tradicional, o professor consegue despertar o interesse até daquele aluno que possui mais dificuldade. Ao se sentir motivado, o discente tem mais capacidade de ultrapassar possíveis barreiras cognitivas.

4.3.2 O material utilizado

Figura 34 – Texto da Atividade 3

Fonte: Elaborado pela autora (vide anexo C)

Foi elaborado um texto pela autora para essa atividade. O texto foi dividido em duas

partes onde, na primeira parte (Figura 34), a personagem Hikari explica a diferença entre código e cifra, menciona os tipos de cifras existentes e exemplifica a cifra simétrica de substituição monoalfabética utilizando a Cifra de César.

Na segunda parte do texto (Figura 35), a personagem utiliza a Cifra de César para explicar como cifrar uma mensagem utilizando chaves numéricas. A necessidade de não usar sempre a mesma chave para que a cifra não seja descoberta facilmente, como foi o caso da Cifra de César, também é mencionada nessa etapa. Quatro itens são propostos como tarefa de cifrar ou decifrar mensagens. No terceiro item, um enigma matemático precisa ser resolvido para se descobrir a chave secreta. E no quarto item, o aluno deverá ser o criptógrafo, criar a mensagem, fazer um enigma para a chave, cifrar a mensagem, enviar para um colega de sua escolha que deverá resolver o enigma e decifrar a mensagem.

Figura 35 – Continuação do Texto da Atividade 3

Continuando...

A Cifra de César foi descoberta pelos inimigos do Império Romano porque César cometeu um grave erro, utilizou sempre a mesma chave para criptografar suas mensagens, três posições à frente, ou seja, chave 3.

Para não cometermos o mesmo erro, vamos fazer uso de chaves diferentes para cada cifragem!

É muito simples, veja como funciona:

Vamos supor que usemos a chave 10 para criptografar a mensagem SOCORRO.

O primeiro passo é escrever todo o alfabeto, iniciando pelo *a* na posição 10 até o *p* na posição 25 e continuando do *q* na posição 0 até o *z* na posição 9:

TEXTO CLARO	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
CHAVE	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
TEXTO CIFRADO	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

Então é só trocar as letras da mensagem pelas letras do alfabeto cifrante. Logo, a mensagem SOCORRO cifrada com a chave 10 é IESEHHE.

Agora é a sua vez, utilize a tabela auxiliar para resolver os exercícios abaixo:

1. Utilizando a chave 22, cifre a mensagem: QUEREMOS PAZ
   _____
2. Utilizando a chave 15, decifre a mensagem: PFEP LXZX FTEZ
   _____
3. Descubra a chave resolvendo o seguinte enigma:
   Sou um múltiplo de 4, antecessor de um número primo e estou entre 14 e 25. Quem sou? _____
   Agora, utilizando a chave encontrada, cifre a mensagem: SALVE O PLANETA
   _____
4. Agora você será o criptógrafo. Crie uma mensagem curta, escolha uma chave, cifre a mensagem e envie para um colega juntamente com um enigma para que ele possa descobrir a chave e decifrar a sua mensagem.

Mensagem criada:_____ Chave:_____

Mensagem cifrada:_____

Enigma: _____

Tabela auxiliar:

TEXTO CLARO	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
CHAVE	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
CIFRA																										

Fonte: Elaborado pela autora (vide anexo C)

4.3.3 Desenvolvimento da atividade

Antes de começar a atividade, se possível, colocar os alunos sentados em círculo. Só então, o professor distribuirá o texto da atividade. Incentivá-los a ler o texto para a turma, esperando que algum deles se interesse pela leitura.

Na primeira parte do texto, o título está criptografado pela Cifra de César e isso vai causar um certo espanto ao tentarem lê-lo, esse é o objetivo! O professor deverá mencionar que o título está criptografado e ao final da atividade todos serão capazes de decifrá-lo.

Chamar a atenção dos alunos para as imagens, elas possuem um papel importante e não devem ser ignoradas. Ilustram explicações dadas por escrito no texto. Ao final da leitura, com o objetivo de esclarecer o conteúdo, fazer as seguintes perguntas:

- O que significa ininteligível?

  Resposta: Que não se pode entender.

- Qual a diferença entre código e cifra?

  Resposta: Código é um sistema no qual toda palavra ou frase de um mensagem é substituída por outra palavra, frase ou símbolo, alterando o sentido da mensagem. Cifra é um sistema onde cada letra da mensagem é trocada por outra letra ou símbolo, necessitando sempre de uma chave para iniciar a cifragem.

- O que é chave?

  Resposta: Chave é uma senha que dará início ao processo de cifragem ou decifragem.

- Qual é a diferença entre cifra de simétrica e cifra assimétrica?

  Resposta: A cifra simétrica utiliza uma única chave conhecida tanto pelo emissor quanto pelo receptor da mensagem, ou seja, há a necessidade de se combinar a chave antes das trocas de mensagens. Já a cifra assimétrica possui dois tipos de chave onde uma é pública, qualquer um pode saber, e a outra é privada, de conhecimento apenas do receptor da mensagem. Não há necessidade de se combinar as chaves para troca de mensagem.

- Como funciona a Cifra de César?

  Resposta: Substituindo cada letra por outra situada a três posições à frente no alfabeto.

- Como se classificam as cifras simétricas de substituição?

  Resposta: Monoalfabéticas ou polialfabéticas.

- Utilizando a Cifra de César, qual é o título do texto decifrado?

  Resposta: CRIPTOGRAFANDO

Através do texto, os alunos devem tentar responder as questões. Caso apresentem dificuldade, o professor deverá intervir esclarecendo as possíveis dúvidas. Se os alunos demonstrarem curiosidade sobre as cifras assimétricas, explicar que, para um estudo mais aprofundado, existe uma necessidade de conhecimentos matemáticos que vão muito além do ano de escolaridade que eles se encontram.

No segundo momento da atividade, utilizaremos a segunda parte do texto. Nessa etapa, o professor esclarecerá o que é uma chave criptográfica e explicar como ela deve ser

utilizada numa cifra simétrica de substituição monoalfabética. O docente não poderá deixar de destacar a importância de manter a chave em segredo e mudá-la sempre que for possível. A respeito do exemplo dado, certificar-se de que o mesmo ficou bem claro e que não resta dúvida no processo de cifragem. Após os esclarecimentos quanto ao exemplo, poderão executar as atividades propostas. Auxiliá-los nessa parte, muitos encontrarão dificuldades enquanto outros acharão extremamente fácil.

Resposta dos exercícios e algumas orientações importantes para um bom aproveitamento da atividade e melhor desempenho:

1. Utilizando a chave 22, cifre a mensagem: QUEREMOS PAZ

   Resposta: uyiviqsw ted

2. Utilizando a chave 15, decifre a mensagem: PFEP LXZX FTEZ

   Resposta: EUTE AMOM UITO, ou seja, EU TE AMO MUITO. O agrupamento das letras, feito de quatro em quatro, foi proposital. Deve ser explicado ao aluno que isso dificulta a decifragem por um intruso, essa técnica é muito utilizada na criptografia.

3. Descubra a chave resolvendo o seguinte enigma: “Sou um múltiplo de 4, antecessor de um número primo e estou entre 14 e 25. Quem sou?” Agora, utilizando a chave encontrada, cifre a mensagem: SALVE O PLANETA.

   Resposta: A chave é 16. Para descobrir a chave, precisará desvendar o enigma que aborda os seguintes conteúdos: múltiplos de 4, números primos e ordem dos números naturais. A cifragem da mensagem é: ckvfo y zvkxodk. Se fossemos enviar essa mensagem para alguém, seria mais seguro agrupar as letras de forma que a letra y não fique sozinha. Por exemplo: ckvf oyzvk xodk.

4. Resposta pessoal

Preenchimento da tabela auxiliar (Figura 36):

Figura 36 – Tabela Auxiliar preenchida

TEXTO CLARO	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
CHAVE	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
CIFRA	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
	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
	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

Fonte: Elaborado pela autora

4.3.4 Concluindo a atividade

Ao final dessa atividade o aluno deverá ser capaz de cifrar e decifrar mensagens utilizando cifras de substituição monoalfabética, e sentindo-se motivado com a realização das tarefas matemáticas.

4.4 Atividade 4 - Cifra Simétrica de Substituição Polialfabética

4.4.1 Objetivos das atividades

A quarta atividade, com duração de aproximadamente 1h e 40 minutos, tem como objetivo principal utilizar o Disco de Alberti para exemplificar o funcionamento de uma cifra simétrica de substituição polialfabética.

Na primeira parte da atividade, o aluno conhecerá o Disco de Alberti e fabricará seu próprio Disco. Para a fabricação do Disco de Alberti, deverão ter conhecimento básico sobre círculo e seus elementos. O professor deverá aproveitar a atividade para ensinar ou revisar tais conceitos.

Já na segunda parte, os alunos resolverão exercícios de cifragem monoalfabética e polialfabética com o Disco de Alberti. Novamente haverá a necessidade de resolver enigmas matemáticos para descobrir as chaves numéricas. Nessa etapa, os conteúdos abordados serão: números naturais, números primos, múltiplos, divisores, MMC, MDC, expressões numéricas envolvendo raiz quadrada e potência e o algoritmo da divisão.

As teorias de Piaget, Freire e Vygotsky, destacam a importância de motivar os alunos utilizando estratégias variadas. A proposta de construção do Disco de Alberti e sua aplicação na realização das atividades é uma excelente estratégia de motivação no processo de aprendizagem.

4.4.2 Material utilizado

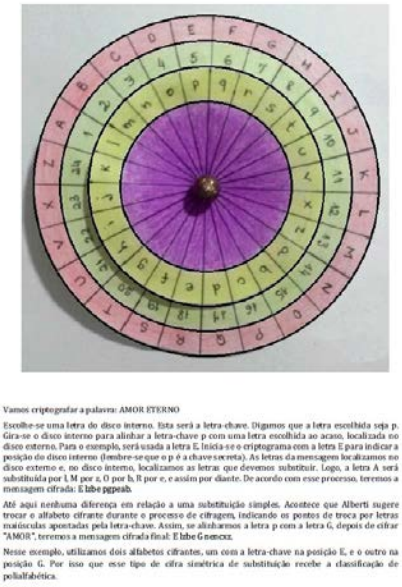
Figura 37 – Texto sobre o Disco de Alberti

Fonte: Elaborado pela autora (vide anexo D)

Na primeira parte da atividade, utilizaremos um texto elaborado pela autora, sobre o Disco de Alberti (Figura 37 e figura 38). Neste, a personagem Hikari dará instruções para que os próprios alunos confeccionem o seu disco. Etapa de relevante importância, pois, ao

construir um instrumento, como o Disco de Alberti, fará com que o aluno se interesse ainda mais pela sua utilização, além de ser um momento de descontração.

Figura 38 – Texto sobre o Disco de Alberti



Vamos criptografar a palavra: AMOR ETERNO

Escolhe-se uma letra do disco interno. Esta será a letra-chave. Digamos que a letra escolhida seja p. Gira-se o disco interno para alinhar a letra-chave p com uma letra escolhida ao acaso, localizada no disco externo. Para o exemplo, será usada a letra E. Inicia-se o criptograma com a letra E para indicar a posição do disco interno (lembre-se que o p é a chave secreta). As letras da mensagem localizamos no disco externo e, no disco interno, localizamos as letras que devemos substituir. Logo, a letra A será substituída por l, M por z, O por b, R por e, e assim por diante. De acordo com esse processo, teremos a mensagem cifrada: E lzbe ggpeab.

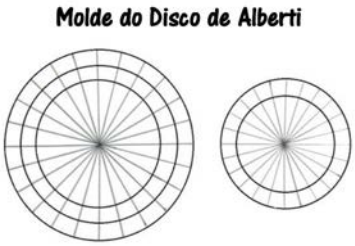
Até aqui nenhuma diferença em relação a uma substituição simples. Acontece que Alberti sugere trocar o alfabeto cifrante durante o processo de cifragem, indicando os pontos de troca por letras maiúsculas apontadas pela letra-chave. Assim, se alinharmos a letra p com a letra G, depois de cifrar "AMOR", teremos a mensagem cifrada final: E lzbe G nemcxx.

Nesse exemplo, utilizamos dois alfabetos cifrantes, um com a letra-chave na posição E, e o outro na posição G. Por isso que esse tipo de cifra simétrica de substituição recebe a classificação de polialfabética.

Fonte: Elaborado pela autora (vide anexo D)

Para a fabricação do disco, os alunos deverão ter em mãos: folha branca A4 ou cartolina, lápis, borracha, régua, compasso, transferidor, tesoura e percevejo ou brinco pequeno com tarraxa. Lápis de cor não é obrigatório, contudo em toda sala de aula sempre existe quem adore colorir, o que fará com que o Disco de Alberti fique ainda mais atrativo, bonito e único, já que cada um pintará a seu modo.

Figura 39 – Molde do Disco de Alberti



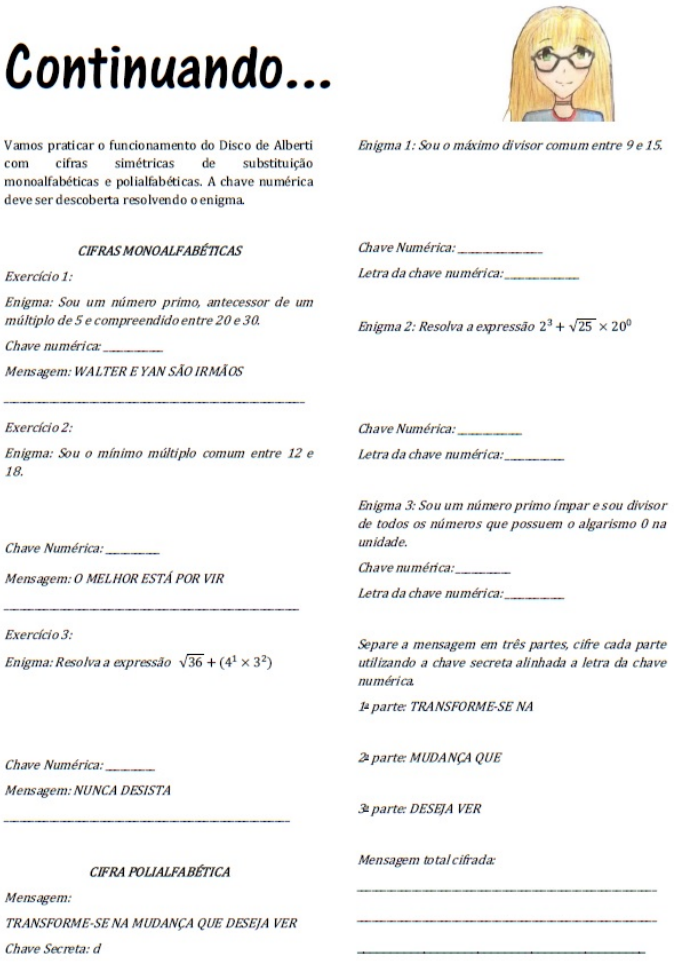
Fonte: Elaborado pela autora (vide anexo D)

Caso a escola não disponha do material necessário, deverá ser solicitado aos discentes com antecedência. Considerando a possibilidade de, ainda assim, não existirem os instrumentos específicos para a construção, o docente poderá utilizar o molde do Disco

de Alberti (Figura 39) que se encontra no anexo juntamente com os demais textos. Assim, os alunos só precisarão preenchê-lo, prendê-lo e colori-lo se quiserem.

Na segunda parte, foram elaborados exercícios de aplicação do dispositivo criptográfico (Figura 40). O professor deverá resolvê-los antes de aplicá-los. Estar seguro do conteúdo é essencial para ministrar uma boa aula. Caso haja alguma dúvida na resolução, basta conferir as respostas dos exercícios que se encontram no desenvolvimento da atividade.

Figura 40 – Exercícios de aplicação do Disco de Alberti



Continuando...

Vamos praticar o funcionamento do Disco de Alberti com cifras simétricas de substituição monoalfabéticas e polialfabéticas. A chave numérica deve ser descoberta resolvendo o enigma.

CIFRAS MONOALFABÉTICAS

Exercício 1:

Enigma: Sou um número primo, antecessor de um múltiplo de 5 e compreendido entre 20 e 30.

Chave numérica: _____

Mensagem: WALTER E YAN SÃO IRMÃOS

Exercício 2:

Enigma: Sou o mínimo múltiplo comum entre 12 e 18.

Chave Numérica: _____

Mensagem: O MELHOR ESTÁ POR VIR

Exercício 3:

Enigma: Resolva a expressão $\sqrt{36} + (4^1 \times 3^2)$

Chave Numérica: _____

Mensagem: NUNCA DESISTA

CIFRA POLIALFABÉTICA

Mensagem:

TRANSFORME-SE NA MUDANÇA QUE DESEJA VER

Chave Secreta: d

Enigma 1: Sou o máximo divisor comum entre 9 e 15.

Chave Numérica: _____

Letra da chave numérica: _____

Enigma 2: Resolva a expressão $2^3 + \sqrt{25} \times 20^0$

Chave Numérica: _____

Letra da chave numérica: _____

Enigma 3: Sou um número primo ímpar e sou divisor de todos os números que possuem o algarismo 0 na unidade.

Chave numérica: _____

Letra da chave numérica: _____

Separe a mensagem em três partes, cifre cada parte utilizando a chave secreta alinhada a letra da chave numérica.

1ª parte: TRANSFORME-SE NA

2ª parte: MUDANÇA QUE

3ª parte: DESEJA VER

Mensagem total cifrada:

Fonte: Elaborado pela autora (vide anexo D)

4.4.3 Desenvolvimento da atividade

Primeiramente, o professor irá distribuir o texto para a leitura, juntamente com a folha A4. Os alunos deverão construir o disco utilizando as instruções do texto e os materiais pedidos. Caso os alunos não tenham condições de trazer todo o material para confecção do disco, o professor poderá utilizar o molde do Disco de Alberti. Atividade de grande valor para

revisar ou conceituar círculo, circunferência, circunferências concêntricas, raio, diâmetro e coroa circular.

Após a confecção do disco e reprodução do exemplo, o professor deverá distribuir a folha de exercícios.

CIFRAS MONOALFABÉTICAS

Exercício 1:

Enigma: Sou um número primo, antecessor de um múltiplo de 5 e compreendido entre 20 e 30.

Chave numérica: 29

Observe que, no Disco confeccionado pelos alunos, a sequência termina no número 24. Os alunos irão questionar, terão dúvidas sobre o que fazer, acharão que o enigma está errado. Como resolver esse problema?

Mostrar aos alunos que é muito simples, bastando continuar a contagem a partir do número 1. O 25 seria 1, o 26 seria 2, o 27 seria 3, o 28 seria 4 e finalmente o 29 seria 5.

É mais prático utilizar o algoritmo da divisão pois, seja o número pequeno ou grande, a chave procurada será sempre o resto da divisão.

Assim temos, $29 \div 24 = 1$ resto 5, ou seja, a chave numérica é 5.

Mensagem: WALTER E YAN SÃO IRMÃOS

Lembre-se de que estamos trabalhando com o Disco de Alberti, mas a cifra é monoalfabética, então basta alinharmos a letra *a* do disco interno com o número 5 e cifrar a mensagem. As letras da mensagem procuramos no disco externo e substituímos pela letra que está alinhada no disco interno. É importante esclarecer que acentos, hífen e cedilha foram desconsiderados na cifragem, somente a letra é cifrada. No caso das letras W e Y, repetimos a própria letra como cifra.

Mensagen cifrada: wuhpan a yuj ouk eniuko

Exercício 2:

Enigma: Sou o mínimo múltiplo comum entre 12 e 18.

M(12) = 0, 12, 24, 36, 48,... M(18) = 0, 18, 36, 54,... MMC(12, 18) = 36

Chave Numérica: O resto da divisão de 36 por 24, ou seja, 12.

Mensagem: O MELHOR ESTÁ POR VIR!

Alinhamos a letra *a* do disco interno com a chave numérica 12 do disco externo. Para cifrar basta seguir o mesmo processo do exercício anterior, localizar as letras da mensagem no disco externo e substituir pelas letras alinhadas no disco interno.

Mensagem cifrada: d braudg rhin edg kvg

Exercício 3:

Enigma: Resolva a expressão $\sqrt{36} + (4^1 \times 3^2)$

$\sqrt{36} + 4^1 \times 3^2 =$

$6 + 4 \times 9 =$

$6 + 36 = 42$

Chave Numérica: 18 (Resto da divisão de 42 por 24)

Mensagem: NUNCA DESISTA

Alinhamos a letra *a* do disco interno com a chave numérica 18 do disco externo e seguimos o mesmo processo dos exercícios anteriores.

Mensagem cifrada: udujh klbpbch

CIFRA POLIALFABÉTICA

Mensagem:

TRANSFORME-SE NA MUDANÇA QUE DESEJA VER

Chave Secreta: d

Nos exercícios das cifras monoalfabéticas, utilizávamos sempre a letra *a* do disco interno alinhada à chave numérica localizada no disco externo. Agora existe uma chave secreta que será utilizada para alinharmos os dois discos.

Enigma 1: Sou o máximo divisor comum entre 9 e 15.

D(9) = 1, 3, 9

D(15) = 1, 3, 5, 15

MDC(9, 15) = 3

Chave Numérica: 3

Letra da chave numérica: C

Enigma 2: Resolva a expressão $2^3 + \sqrt{25} \times 20^0$

$2^3 + \sqrt{25} \times 20^0 =$

$8 + 5 \times 1 =$

$8 + 5 = 13$

Chave Numérica: 13

Letra da chave numérica: M

Enigma 3: Sou um número primo ímpar e sou divisor de todos os números que

possuem o algarismo 0 na unidade.

Chave numérica: 5

Letra da chave numérica: E

Separe a mensagem em três partes, cifre cada parte utilizando a chave secreta d alinhada a letra da chave numérica encontrada em cada enigma.

$1^{\underline{a}}$ parte: TRANSFORME-SE NA

Alinhar a chave secreta d do disco interno, com a letra C (letra da chave numérica) do disco externo. Sempre inicia-se a cifragem com a letra da chave numérica.

Mensagem cifrada: C usbotgpsnf tf ob

$2^{\underline{a}}$ parte: MUDANÇA QUE

Alinhar a chave secreta d do disco interno, com a letra M (letra da chave numérica) do disco externo. Sempre inicia-se a cifragem com a letra da chave numérica.

Mensagem cifrada: M dlsperp hlt

$3^{\underline{a}}$ parte: DESEJA VER

Alinhar a chave secreta d do disco interno, com a letra E (letra da chave numérica) do disco externo. Sempre inicia-se a cifragem com a letra da chave numérica.

Mensagem cifrada: E cdrdiz udq

Mensagem total cifrada: C usbotgpsnf tf ob M dlsperp hlt E cdrdiz udq

4.4.4 Concluindo a atividade

Mostrar ao aluno que foram utilizados três alfabetos cifrantes na cifragem polialfabética e que a dificuldade de decifragem dessa mensagem é muito maior que das cifras monoalfabética.

Esclarecer que, atualmente, essas cifras já são muito simples de serem decifradas porém, na época em que foram criadas, eram consideradas impossíveis de serem quebradas.

Ao final dessa atividade o aluno deverá ser capaz de cifrar uma mensagem utilizando o Disco de Alberti, sabendo identificar a diferença entre cifras monoalfabéticas e polialfabéticas.

O professor poderá utilizar enigmas abordando outros conteúdos, de acordo com a sua necessidade e o ano de escolaridade em que se está trabalhando. O professor também poderá empregar essa atividade como inspiração para montar uma outra semelhante, com foco em outros conteúdos matemáticos e levando em consideração o desenvolvimento cognitivo do aluno.

Capítulo 5

Considerações Finais

O contexto atual da criptografia, as possibilidades de aplicação matemática aliadas à carência de material didático voltado ao Ensino Fundamental, sobretudo por se tratar de um assunto fascinante, foram alguns dos fatores que impulsionaram o presente estudo.

Alcançamos nosso objetivo ao desenvolver atividades voltadas para o ensino fundamental, utilizando a criptografia e as cifras simétricas, possibilitando a abordagem de conteúdos matemáticos diversos, com o intuito de complementar o trabalho do professor LOUREIRO (2014). Além das atividades, temos nos apêndices deste trabalho, cinco textos sobre assuntos relacionados à criptografia, com o objetivo de aprimorar o conhecimento do professor sobre o tema, bem como, servir de fonte de pesquisa para elaboração de uma aula diferenciada.

Esperamos ter contribuído para a docência dos professores de matemática e também como fonte de pesquisa e inspiração para novos estudos dentro deste mesmo tema. Criar novas atividades utilizando criptografia, aplicá-las em sala de aula e analisar seus resultados, tendo como foco o desenvolvimento cognitivo do aluno, são opções de complementação para esta pesquisa. Ainda há muito o que explorar, a Criptografia é uma fonte de inúmeras possibilidades de estudo e ideias.

Assim, ao implementarmos; lúdica, dinâmica, atual e prazerosamente; a abordagem de conteúdos , através da criptografia, concluímos sobre a possibilidade de uma prática de ensino voltada para a realidade de vida do discente, atendendo as suas necessidades.

Diante do resultado obtido, atuará como catalisador para outras iniciativas comprometidas com as mudanças sócio-político-econômicas que vão ao encontro deste estudante da segunda década do terceiro milênio.

Referências

BRASIL. *Parâmetros Curriculares Nacionais: Ensino Fundamental - Matemática*. Brasília, DF, 1998. Citado na página 18.

BROWN, D. *O Código Da Vinci - Edição Especial Ilustrada*. [S.l.: s.n.], 2005. Citado 3 vezes nas páginas 80, 81 e 82.

BRUINI, E. da C. *Aprendizagem Significativa*. 2015. Acessado em 10 de maio de 2016. Disponível em: <http://educador.brasilescola.uol.com.br/trabalho-docente/aprendizagem-significativa.htm>. Citado 2 vezes nas páginas 49 e 50.

CERQUEIRA, D. S. *Estratégias Didáticas para o Ensino da Matemática*. 2013. Acessado em 21 de maio de 2016. Disponível em: <http://revistaescola.abril.com.br/fundamental-2/atividades-didaticas-matematica-752650.shtml?page=0>. Citado na página 50.

COUTINHO, S. C. *Números inteiros e Criptografia RSA*. [S.l.]: Rio de Janeiro, 2000. Citado na página 116.

FERNADES, E. *David Ausubel e a aprendizagem significativa*. 2012. Acesso em 23 de novembro de 2015. Disponível em: <http://revistaescola.abril.com.br/formacao/david-ausubel-aprendizagem-significativa-662262.shtml>. Citado na página 49.

FERRARI, M. *Grandes Pensadores*. 2008. Acesso em 14 de janeiro de 2016. Disponível em: <http://revistaescola.abril.com.br/pensadores/>. Citado 4 vezes nas páginas 41, 44, 45 e 46.

FIARRESGA, V. M. C. *Criptografia e Matemática*. Dissertação (Mestrado) — Universidade de Lisboa, 2010. Citado 2 vezes nas páginas 19 e 22.

FREIRE, P. *Educação e Mudança*. [S.l.: s.n.], 1979. Citado na página 39.

FREIRE, P. *O Educador da Liberdade*. [S.l.]: Outubro, 1988. Citado na página 44.

FREIRE, P. *Pedagogia da autonomia: saberes necessários à prática educativa*. [S.l.: s.n.], 1996. Citado na página 45.

KLUBER, T. E.; BURAK, D. *A Fenomenologia e suas Contribuições para a Educação Matemática*. 2008. Paraná. Acessado em 25 de maio de 2016. Disponível em: <http://www.revistas2.uepg.br/index.php/praxiseducativa/article/viewFile/346/518>. Citado 2 vezes nas páginas 55 e 56.

LOUREIRO, F. O. *Tópicos de criptografia para o ensino médio*. Dissertação (Mestrado) — Universidade Estadual Norte Fluminense, 2014. Citado 8 vezes nas páginas 19, 20, 30, 37, 38, 58, 75 e 114.

MATSUMOTO, M. S. *Despertando o interesse do aluno pela matemática com a criptografia*. Dissertação (Mestrado) — Universidade Federal da Grande Dourados, 2014. Citado 3 vezes nas páginas 19, 20 e 21.

MIRANDA, C. *Leonardo Da Vinci - O homem de todos os códigos*. 2006. Acesso em 13 de abril de 2016. Disponível em: <http://guiadoestudante.abril.com.br/aventuras-historia/leonardo-vinci-homem-todos-codigos-434694.shtml>. Citado na página 82.

NOE, M. *O ensino da Matemática sob a visão de Piaget*. 2015. Acessado em 23 de janeiro de 2016. Disponível em: <http://educador.brasilescola.uol.com.br/estrategias-ensino/o-ensino-matematica-sob-visao-piaget.htm>. Citado na página 41.

NOGUEIRA, C. M. I. *As teorias de aprendizagem e suas implicações na aprendizagem da matemática*. 2007. Acessado em 16 de fevereiro de 2016. Disponível em: <http://periodicos.uem.br/ojs/index.phd/ActaSciHumanSocSci/article/view/141>. Citado 2 vezes nas páginas 47 e 48.

PAGANOTTI, I. *Vygotsky e o conceito de zona de desenvolvimento proximal*. 2011. Acessado em 20 de janeiro de 2016. Disponível em: <http://revistaescola.abril.com.br/formacao/formacao-continuada/vygotsky-conceito-zona-desenvolvimento-proximal-629243.shtml>. Citado na página 43.

PELLEGRINI, D. *Aprenda com eles e ensine melhor*. 2001. Acessado em 20 de novembro de 2015. Disponível em: <http://revistaescola.abril.com.br/formacao/aprenda-eles-ensine-melhor-423205.shtml>. Citado 2 vezes nas páginas 39 e 40.

PRODANOV, C. C.; FREITAS, E. C. *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico*. [S.l.]: Rio Grande do Sul, 2013. Citado 2 vezes nas páginas 56 e 57.

SIEMENS, G. *Conectivismo - Uma Teoria de Aprendizagem para a Idade Digital*. 2004. Acessado em 10 de maio de 2016. Disponível em: <http://pt.slideshare.net/quimicadobruno/conectivismo-uma-teoria-para-a-era-digital>. Citado 2 vezes nas páginas 52 e 53.

SILVA, A. L. S. da. *Mapas Conceituais no Processo de Ensino-Aprendizagem: aspectos práticos*. 2012. Acessado em 23 de Maio de 2016. Disponível em: <http://www.infoescola.com/pedagogia/mapas-conceituais-no-processo-de-ensino-aprendizagem-aspectos-praticos/>. Citado na página 50.

SILVA, E. L.; MENEZES, E. M. *Metodologia da Pesquisa e Elaboração de Dissertação*. [S.l.]: Florianópolis, 2005. Citado 4 vezes nas páginas 54, 55, 57 e 58.

SINGH, S. *O livro dos Códigos*. [S.l.: s.n.], 2001. Citado 4 vezes nas páginas 34, 35, 36 e 37.

TKOTZ, V. *Criptografia - Segredos Embalados para Viagem*. [S.l.: s.n.], 2005. Citado 11 vezes nas páginas 16, 17, 21, 23, 24, 25, 27, 29, 31, 32 e 34.

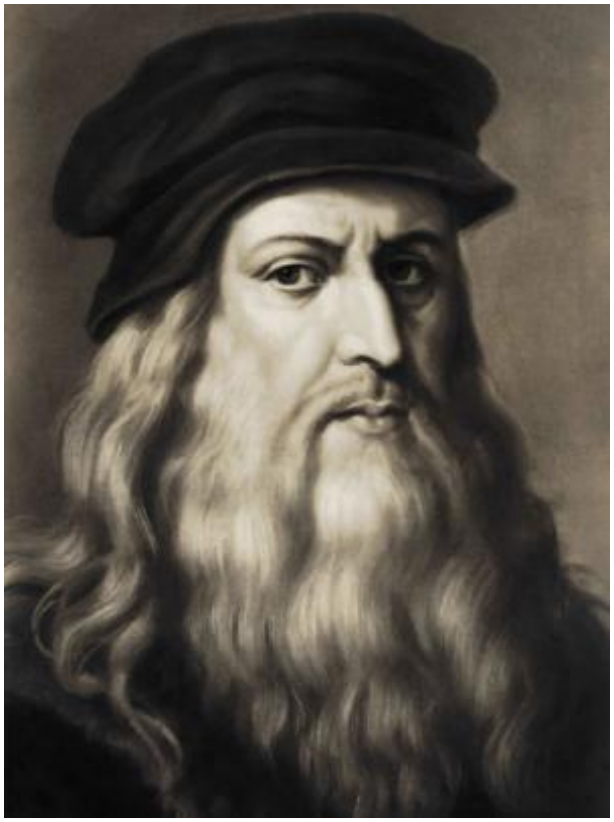
Apêndices

APÊNDICE A

Lenda ou realidade - O misterioso Críptex

A Criptologia é uma ciência que há muito tempo encanta com seus mistérios e histórias intrigantes, dignas de livros e filmes. Uma dessas histórias chamou a atenção de um grande escritor atual por envolver o nome de um dos maiores gênios da humanidade, o grande cientista, matemático, engenheiro, inventor, anatomista, pintor, escultor, arquiteto, botânico, poeta e músico, Leonardo Da Vinci (1452–1519).

Figura 41 – Leonardo Da Vinci



Fonte: https://www.codeavengers.com/c/gabrielj/leonardodavinci.html

Um cofre, supostamente desenhado por Da Vinci (Figura 41), ganhou fama no mundo através do livro e do filme de Dan Brown - O Código Da Vinci. Esse cofre foi batizado por Dan Brown de críptex. Essa palavra foi feita da fusão de outras duas palavras: criptologia e códice (codex)[1].

O críptex tem a forma de um cilindro, sua tranca é feita por um conjunto de cinco anéis com todas as letras do alfabeto gravadas para efetuar a senha e abri-lo. O objetivo de um críptex é esconder uma mensagem de tal forma que somente a senha é capaz de revelá-la, abrindo o críptex. Qualquer tentativa de abri-lo à força bruta, resulta na destruição imediata de seu conteúdo. São $26^5 = 11881376$ de senhas possíveis (BROWN, 2005, p.185). Pouco se sabe sobre a veracidade do críptex, porém uma cópia fiel encontra-se atualmente no museu do Louvre. (Figura 42)

Figura 42 – Réplica do críptex

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

“A maioria das invenções não confeccionadas de Da Vinci jamais fora estudada nem tinha nome. O termo "críptex" podia ter sido inclusive inventado por seu avô, um nome adequado para aquele dispositivo que empregava a criptologia para proteger informações no rolo, ou códex, no seu interior”. (BROWN, 2005, p.183)

Segundo Dan Brown (Figura 43), no livro O Código da Vinci, na página que antecede o prólogo, “Todas as descrições de obras de arte, arquitetura, documentos e rituais secretos neste romance correspondem rigorosamente à realidade”. Sendo assim, sobre o críptex, presumimos que "o desenho original se encontra em um dos diários secretos de Da Vinci"

[1] Os códices (ou codex, da palavra em latim que significa "livro", "bloco de madeira") eram os manuscritos gravados em madeira, em geral do período da era antiga tardia até a Idade Média. Manuscritos do Novo Mundo foram escritos por volta do século XVI. O códice é um avanço do rolo de pergaminho, e gradativamente substituiu este último como suporte da escrita. O códice, por sua vez, foi substituído pelo livro.

(BROWN, 2005, p.183). Em O Código Da Vinci, Dan Brown não se utiliza apenas do críptex para fazer uso da criptologia, encontramos também mensagens utilizando cifra de transposição na página 185 e a cifra de substituição hebraica - Atbash - na página 275.

Figura 43 – Dan Brown

Fonte: http://www.danbrown.com/author-section

No capítulo 47 de O Código Da Vinci, o personagem Langdon descreve com detalhes o artefato.

"Feito de mármore branco polido, tratava-se de um cilindro de pedra aproximadamente com as mesmas dimensões de uma lata de bolas de tênis. Mais complexo do que uma única coluna de pedra, o cilindro parecia, porém, ter sido montado de várias peças. Cinco discos feitos de mármore do tamanho de uma rosquinha grande haviam sido empilhados e presos um ao outro dentro de uma delicada armação de metal. Parecia algum tipo de caleidoscópio cheio de rodas. Cada extremidade do cilindro estava fechada com uma tampa, também de mármore, tornando impossível ver o interior. Depois de ouvir o barulho de um líquido, Langdon presumiu que o cilindro fosse oco. Por mais intrigante que pudesse ser a composição do cilindro, foram, porém, as gravações em volta do tubo que primeiro chamaram sua atenção. Em cada um dos cinco discos havia sido gravada a mesma série improvável de letras – o alfabeto inteiro". (BROWN, 2005, p.182)

Também nesse capítulo a personagem Sophie explica o curioso passatempo do seu avô - criar modelos das invenções de Da Vinci.

"Até mesmo um exame superficial dos diários de Da Vinci revelava por que o luminar era tão famoso por sua falta de continuidade quanto era por seu brilhantismo. Da Vinci havia desenhado projetos de centenas de invenções que jamais construíra. Um dos passatempos preferidos de Jacques Saunière era dar vida às mais obscuras elucubrações de Da Vinci – ampulhetas, bombas d'água, críptex, e até um modelo inteiramente articulado de um cavaleiro medieval francês, que colocara, cheio de orgulho, em cima de sua escrivaninha no escritório". (BROWN, 2005, p.183)

Dan Brown, através de seus personagens, menciona Da Vinci como o precursor da criptologia. E de fato, Leonardo Da Vinci, com a preocupação de proteger suas criações de possíveis espiões, escrevia seus textos da direita para esquerda. Dessa forma, somente com o auxílio de um espelho seus textos poderiam ser lidos. Ele também usava um tipo de taquigrafia muito estranha, na qual utilizava parte de palavras ou símbolos, e não letras, para exprimir ideias. (MIRANDA, 2006)

"Da Vinci havia sido pioneiro da ciência da criptologia, segundo Sophie sabia, embora raramente recebesse crédito por isso. Os professores Universitários de Sophie(...)não mencionavam que tinha sido Leonardo quem inventara uma das formas mais rudimentares de criptografia séculos antes". (BROWN, 2005, p.183)

Figura 44 – Texto de Da Vinci escrito da direita para esquerda

Fonte: http://criptografia2011.blogspot.com.br/2011/09/leonardo-da-vinci.htm

São muitas curiosidades, excentricidades e muitos mistérios que cercam a vida e a obra de Leonardo Da Vinci. São muitas histórias e suposições a respeito de códigos secretos em suas pinturas. Contudo, somente podemos afirmar que Leonardo Da Vinci, esse gênio incrível, sempre inquietou a mente dos mais curiosos e até hoje mexe com o imaginário de todos nós.

APÊNDICE B

Hackers e Crackers

Esses termos são comuns na área de informática, mas geram bastante confusão. Muita gente acha que hacker (a palavra hack foi criada na década de 50 para descrever modificações inteligentes em relés eletrônicos) e cracker (cracking = quebra) significam a mesma coisa. Na verdade, o termo hacker significa alguém que muda alguns programas através de técnicas simples e inteligentes com intuito de melhorar esses programas. Normalmente o hacker é uma pessoa do lado bom enquanto que o cracker é uma pessoa sem ética ou escrúpulos. Os hackers e crackers são pessoas inteligentes, porém, enquanto os hackers usam sua inteligência para o bem, os crackers a usam para o mal.

Existem diversos relatos de sites que são invadidos diariamente pelos crackers. Na maioria das vezes quando um site é invadido, são colocadas mensagens ofensivas (muitas vezes relativas à política) nesses sites com “assinaturas” do cracker que invadiu o sistema. O pentágono e o FBI nos Estados Unidos já foram invadidos por crackers diversas vezes. Os prejuízos são incalculáveis. Ao se invadir um site, o cracker assume um determinado nível de controle desse site que pode ser parcial ou total. Se a invasão for total, com certeza o prejuízo será muito maior. Muitos hackers são contratados por sites para que descubram vulnerabilidades que crackers poderão utilizar para invadir esses sites. Nesse caso, o hacker está realizando uma boa ação pois está ajudando o site a se tornar mais seguro.

Muitos crackers se tornam hackers após serem pegos e punidos. Ir para o “lado claro da força” na maioria das vezes, é mais compensador. Mas o que os crackers ganham ao invadir sites e prejudicar a vida de muita gente? Os crackers ganham poder, fama e dinheiro. Ao roubar contas bancárias, números de cartão de crédito, informações confidenciais, projetos secretos, projetos de produtos que serão lançados no mercado, dados pessoais e outras informações valiosas, o cracker assume o poder e começa a subornar as vítimas, pedindo dinheiro em troca dessas valiosas informações roubadas. Por ter um conhecimento computacional enorme, fica difícil apanhar esses crackers pois eles vão se superando a cada dia.

O interesse crescente na Criptografia, ciência empregada ao longo da história para

proteger segredos políticos e militares, tornou-se um elemento crucial do cotidiano numa era em que um número crescente de indivíduos tem pelo menos duas senhas: uma para acessar sua conta bancária em caixas eletrônicos e outra para abrir seu e-mail.

A busca de códigos imunes a hackers e crackers, os criptoanalistas da internet, usa equações matemáticas cada vez mais complexas. Delas dependem não só grandes negócios mas qualquer operação comercial na internet.

Os fabricantes de sistemas de segurança estão deixando de lutar contra os "quebradores de códigos". Eles preferem ter a colaboração deles, usando-os como pilotos de prova criptográficos. Você sabe: se não é possível vencer seu inimigo, junte-se a ele. Sinal dos tempos. Divulgar para melhor guardar um segredo.

Até os anos 70, ambos, o algoritmo e a chave, costumavam ser mantidos em sigilo. Hoje as empresas divulgam os algoritmos e até oferecem prêmios em dinheiro para cientistas e hackers de plantão "quebrarem" seus sistemas – ou seja, encontrarem as chaves. Se ninguém consegue, mesmo sabendo o algoritmo, significa que ele é bom mesmo.

Um desses casos ficou marcado na história da decifração na Criptografia. Em 1998, para testar a segurança da nova cifra chamada de ECC (técnica testada para tornar invioláveis as ligações na telefonia celular digital), a empresa canadense Certicom lançou como desafio a quebra dessa cifra. A equipe de pesquisadores do Instituto Nacional de Informática da França, chefiada pelo especialista Robert Harley anunciou ter decodificado uma mensagem cifrada em ECC. A equipe já conhecia o tipo da chave que abriria o "cadeado" da cifra. A estratégia usada foi desenvolver um programa para "fabricar chaves" e, assim, produzir todas as chaves possíveis daquele "tipo". Cada uma foi testada. Durante quatro meses, 9 500 computadores fabricaram um número incalculável de chaves. Cerca de 1 300 voluntários, em quarenta países, trabalharam até achar a chave certa. A Certicom pagou um prêmio de 10 000 dólares aos autores da façanha.

Para proteger suas informações pessoais a escolha das senhas é uma questão de Matemática e não de gosto. Para garantir a privacidade, é necessário prestar atenção nos caracteres escolhidos para compor sua senha pessoal. Para alguém descobri-la, será preciso testar todas as combinações possíveis. Vamos supor que a senha seja de cinco caracteres. Se você escolhe só números, são 100 000 alternativas; só letras, quase 12 milhões. Mas, se você misturar todos os símbolos presentes no teclado (letras, números e sinais), serão nada menos que 8 bilhões de possibilidades.

As mídias ainda veem os crackers como superespiões com tecnologia a sua disposição. Alguns os chamam de heróis, outros os ultrajam como nada além de criminosos com um pouco de conhecimento técnico. Esta lista é uma introdução de alguns dos crackers/hackers mais famosos da história. Mas no final das contas, os melhores são os únicos que nós nunca ouviremos falar, porque eles nunca serão pegos.

Kevin Mitnick

Também conhecido com Condor, é um dos mais famosos crackers de todos os tempos. Em 1990, Kevin Mitnick (Figura 45) chegou a roubar 20 mil números de cartões de crédito e assombrava o sistema telefônico dos EUA. Condor foi o primeiro cracker a entrar para a lista dos 10 criminosos mais procurados pelo FBI. Ele foi condenado por hackear o sistema do DEC, e teve um merecido tempo na prisão e um período de liberdade supervisionada. Quando se aproximava o fim do período de liberdade hackeou os sistemas e fugiu antes de ser pego. Permaneceu em liberdade por uns 2 anos, até sua prisão em fevereiro de 1995. Foi liberado após 5 anos depois de pagar fiança. Nos primeiros três anos de liberdade não pode conectar-se a internet. Foi lançado em 2000, nos Estados Unidos, o filme Caçada Virtual (no original em Inglês *Takedown*) que conta a história desse famoso hacker. Hoje, Mitnick é um consultor de segurança digital, tendo participado inclusive do evento Campus Party 2010 no Brasil.

Figura 45 – Kevin Mitnick

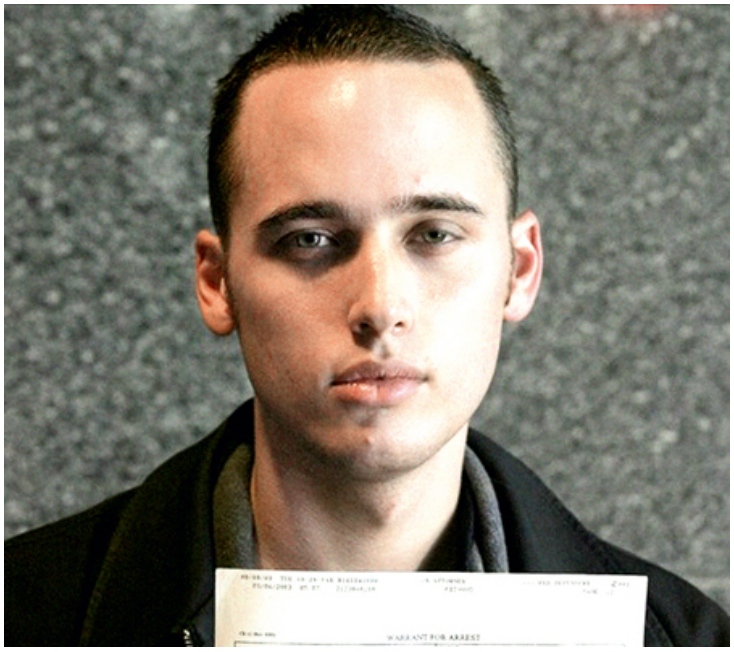
Fonte: http://www.nndb.com/people/448/000022382/kevin-mitnick-2-sized.jpg

Adrian Lamo

Na lista de invasões do jovem cracker americano estão os sites da Microsoft, do Yahoo! e do jornal The New York Times. Titulado como “O Hacker Sem Casa” porque, geralmente, “trabalha” em cybercafes, prédios abandonados e bibliotecas. Em fevereiro de 2002, Adrian Lamo (Figura 46) invadiu o sistema do The New York Times, onde pode ver

todo tipo de dados, por este ato foi preso imediatamente. Sendo condenado a 6 meses de prisão domiciliar na casa de seus pais, 2 anos de cadeia e a pagar 65 mil dólares.

Figura 46 – Adrian Lamo



Fonte: http://www.letsweekly.com/uploads/130819/1-130Q911505T58.jpg

Raphael Gray

Figura 47 – Raphael Gray

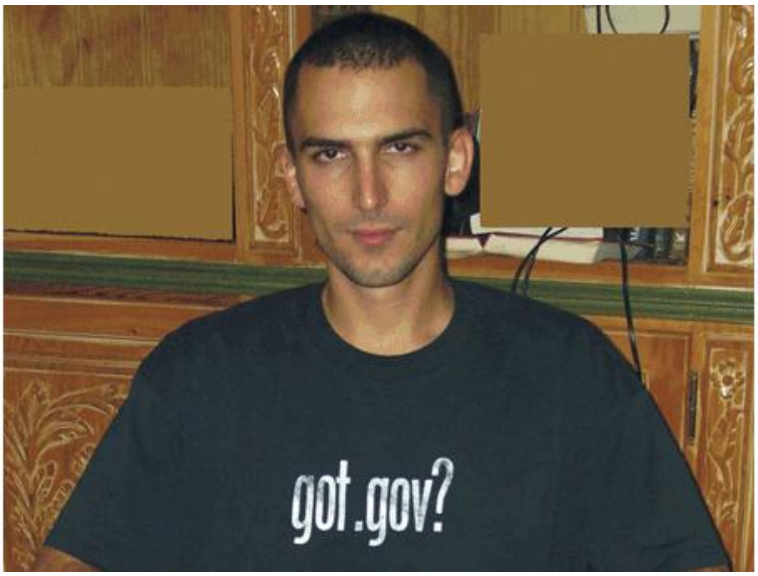
Fonte: http://news.bbc.co.uk/olmedia/1285000/images/_1287754_gray300.jpg

Cracker britânico Raphael Gray (Figura 47), foi condenado com apenas 19 anos por roubar 23 mil números de cartões de crédito, entre eles um de Bill Gates. Usando dados de cartões de crédito roubados, Gray criou dois sites, o "ecrackers.com" e o "freecreditcards.com", onde publicou informações de cartões de crédito roubados de páginas de e-commerce, incluindo o número que ele alegou ser do cartão de crédito de Bill Gates, com o telefone da casa do milionário. O fato chamou a atenção do FBI, que o prendeu em março de 1999.

Jonathan James

Também conhecido como Comrade, foi o primeiro adolescente a ser preso por crimes digitais nos Estados Unidos, em 1999, na época com 16 anos. Aos 15 anos ele invadiu o Departamento de Segurança dos EUA (DTRA), agência responsável por reduzir a ameaça de armas nucleares, biológicas e químicas no país e no estrangeiro. Comrade, também entrou no sistema da NASA. James suicidou-se em maio de 2008, e junto com o corpo foi encontrada uma carta com 5 páginas, justificando que ele não acreditava mais no sistema judiciário. Isso porque ele estava sendo investigado pelo Serviço Secreto por ter ligação - ao qual ele negava - a um grande roubo de dados de clientes de várias lojas virtuais norte-americanas em 2007. Jonathan James (Figura 48) causou um prejuízo de 41 mil dólares pela DTRA e 1.7 milhões de dólares pela NASA.

Figura 48 – Jonathan James



Fonte: http://top10mais.org/wp-content/uploads/2013/10/jonathan-james-nasa.jpg

Jon Lech Johansen

Conhecido como DVD Jon, o cracker norueguês ganhou fama aos 16 anos após burlar os sistemas de proteção dos DVDs comerciais. Tais códigos eram usados pela indústria cinematográfica de Hollywood para impedir que o conteúdo seja reproduzido em áreas diferentes das de venda. Hollywood pediu a prisão do jovem Jon Johansen (Figura 49). Seus pais foram processados em seu lugar, afinal, ele tinha apenas 15 anos, mas foram absolvidos Os defensores do hacker norueguês mantêm várias páginas na internet onde afirmam que não era intenção do menino criar um programa de pirataria de DVDs. O objetivo não teria sido copiar, mas apenas poder assistir aos filmes no sistema operacional Linux, que não possui programas licenciados para rodar DVDs. Ao que parece, Johansen trabalha para quebrar os sistemas anticópias do Blu-Ray, os discos que sucederam os DVDs.

Figura 49 – Jon Johansen

Fonte: https://assets.entrepreneur.com/content/16x9/822/jon-lech-johansen-aka-dvd-jon-starting-up-self-taught-engineer.jpg

Vladimir Levin

Figura 50 – Vladimir Levin

Fonte: http://www.fatosdesconhecidos.com.br/wp-content/uploads/2015/09/64.jpg

Formado pela Universidade de Tecnologia de St.Petesburg, Rússia, esse hacker russo foi o cérebro de um ataque aos computadores do Citybank, em 1994. Com o acesso à rede bancária, ele desviou 10 milhões de dólares de contas de clientes. Vladimir Levin (Figura 50) foi preso pela Interpol em Londres, no Aeroporto de Heathrow, em 1995.

Onel de Guzman

Com apenas 23 anos, o estudante filipino Onel Guzman (Figura 51), criou o famoso vírus "I love you", que era enviado por e-mail com um arquivo anexo chamado "Love-the-letter-for-you". Após a execução, o vírus fazia com que a mensagem fosse enviada para todos os contatos da vítima, e além de se retransmitir, o vírus subscrevia alguns arquivos e infectava vários outros, fazendo com que o malware fosse executado toda vez que a pessoa tentasse abrir um arquivo MP3, por exemplo. Estima-se que o "I love you" tenha sido enviado a mais de 84 milhões de pessoas, causando um prejuízo total de 8,7 bilhões. O estudante filipino que enviou o vírus o fez por pura birra, já que tratava-se de um trabalho de faculdade rejeitado. Ele foi absolvido por faltar legislação que envolvesse crimes digitais em seu país, e também por não terem encontrado provas.

Figura 51 – Onel de Guzman

Fonte: http://ww3.hdnux.com/photos/10/50/03/2261238/5/920x920.jpg

Kevin Poulsen

Esse americano da Califórnia é atualmente diretor do site Security Focus e editor sênior da Wired News. Kevin Lee Poulsen (Figura 52), também conhecido como escuro Dante, ficou famoso quando ganhou um Porsche em um concurso realizado por uma rádio americana, em 1990. O $102^{º}$ ouvinte que telefonasse para a emissora, levava o carro. Poulsen invadiu a central e conseguiu o prêmio. No entanto, foi seu hacking em vários sistemas Federais que atraíram a atenção do FBI e levaram a sua prisão em 1991.

Figura 52 – Kevin Poulsen

Fonte: https://www.soldierx.com/system/files/hdb/Kevin_Poulsen.jpg

Robert Morris

Figura 53 – Robert Morris

Fonte: https://pdos.csail.mit.edu/archive/rtm/morris300.jpg

Esse americano, filho do cientista chefe do Centro Nacional de Segurança Computacional dos EUA, espalhou o primeiro Worm que infectou milhões de computadores e fez grande parte da Internet entrar em colapso, em 1988. Robert Morris (Figura 53) foi o primeiro a ser condenado pela lei de Abuso e Fraude de Computadores dos Estados Unidos,

mas nem cumpriu a pena. Atualmente ele é considerado o mestre dos criadores de pragas virtuais e está trabalhando como professor efetivo do MIT no Laboratório de Inteligência Artificial.Causou um dano de 263500 dolares.

David L. Smith

Smith é o autor do notório "worm Melissa", responsável por derrubar servidores de grandes empresas, como Intel, Lucent e Microsoft e tirar do ar vários servidores de e-mail em 1999. David Smith (Figura 54) foi detido e condenado em 2002 a 10 anos de prisão por ter causado mais de 80 milhões de dólares de prejuízo. A pena chegou a ser reduzida para 20 meses (mais multa de 5 mil dólares) quando Smith aceitou trabalhar com o FBI, logo após sua captura. Inicialmente ele trabalhou 18 horas por semana, mas logo a demanda aumentou, fazendo-o trabalhar 40 horas semanais. Ele foi incumbido de obter conexões entre os autores de vírus novos, mantendo a atenção às vulnerabilidades dos softwares e contribuindo para a captura dos invasores.

Figura 54 – David Smith

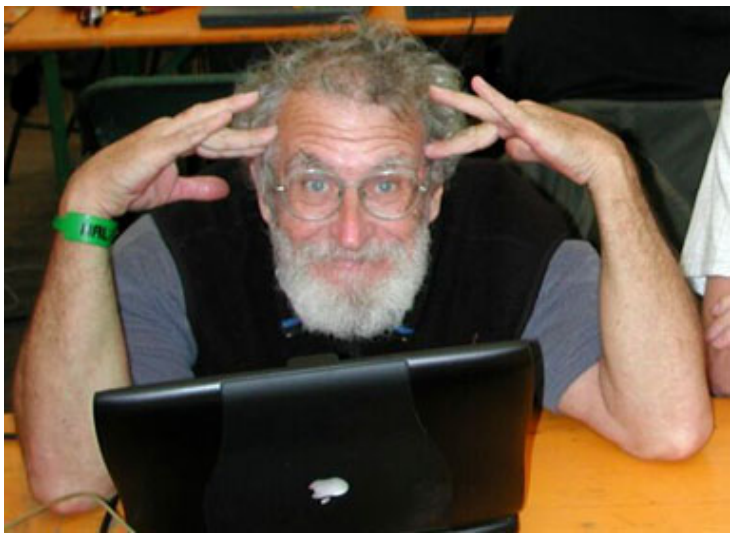
Fonte: http://rockntech.com.br/wp-content/uploads/2014/03/maiores-hackers-existiram_10.jpg

John Draper

Também conhecido como Captain Crunch, John Draper (Figura 55) começou sua “carreira” quando foi informado por um amigo que um apito de brinquedo, que era dado em caixas de cereais do Captain Crunch, emitia um tom de 2600 hertz. Este tom era uma frequência utilizada na fabricação de telefones e conduziu Draper a criar “blue boxes”, dispositivos capazes de reproduzir outros tons de discagem, fazendo ligações de graça. Então aqui estava o homem que poderia fazer ligações gratuitas graças a um brinquedo de caixa de cereal. No meio dos anos 70, ele ensinou algumas habilidades aos cofundadores da Apple, Steve Jobs e Steve Wozniak. Draper ficou empregado temporariamente na Apple, e escreveu o código do EasyWriter, o primeiro processador de texto do Apple II. Draper foi

preso em 1972, sendo condenado a 5 anos.

Figura 55 – John Draper



Fonte: http://tecnologia.culturamix.com/blog/wp-content/uploads/2012/10/john-draper-1.jpg

João Sperandio Neto

Figura 56 – João Sperandio Neto

Fonte: https://www.oficinadanet.com.br/imagens/post/5960/td_sperandio_neto.jpg

É considerado um gênio do mundo virtual. Começou aos 15 anos por diversão. Já ajudou a polícia a prender um pedófilo criando um software que lista todas as imagens que se encontram no computador do usuário. João Neto também usou este talento para cometer fraudes milionárias. Em 2010, aos 24 anos, foi preso pela Polícia Civil de São Paulo por extorsão. O jovem exigiu 500 mil dólares para não desviar 2 milhões de dólares de um banco. João admitiu que invadiu a rede, mas alegou que realizou para mostrar a deficiência

e para tentar um emprego na instituição. A investigação mostra que, em menos de dez dias, desviou 2,2 milhões de reais para as contas de 28 pessoas. Ele alega que já foi sequestrado cinco vezes, e forçado a usar os conhecimentos de informática para beneficiar criminosos. Neto se diz arrependido e afirma que quer usar o dom que tem para ajudar as instituições financeiras e a polícia a combater as fraudes eletrônicas.

Fontes:

http://super.abril.com.br/tecnologia/o-segredo-da-criptografia

http://homesecurity.net/hackers-crackers/

http://lista10.org/diversos/os-10-crackers-mais-famosos-e-seus-feitos-criminosos/

http://www.infoescola.com/informatica/hackers-e-crackers/

http://www.techtudo.com.br/noticias/noticia/2011/06/top-10-os-maiores-hackers-da-historia.html

APÊNDICE C

A criptografia como protagonista

Em vários filmes e livros, a Criptografia é a protagonista da trama. São histórias repletas de mistério, ação e suspense. Nesse capítulo, o objetivo é fornecer ao professor de matemática algumas dicas de filmes, livros que falam sobre criptografia, com o intuito de serem utilizados nas aulas de matemática.

O professor pode levar um filme para assistir com os alunos na escola ou fazer a leitura da síntese de um livro. Podem combinar um delicioso lanche para o final, basta cada um levar algo para comer e beber, transformando o momento num maravilhoso evento. É importante que o professor converse com os alunos a respeito da história, incentive um debate sobre o assunto possibilitando a troca de opiniões. Dessa forma, esse momento irá fornecer muito mais que lazer para os discentes, irá cativá-los para o universo matemático, aproximá-los ainda mais do professor e também uns dos outros, transformando-os em seres humanos ainda mais críticos e proporcionando um crescimento cognitivo para o aluno.

Segue abaixo, algumas sugestões de filmes e livros que abordam o tema criptografia:

FILMES

Códigos de Guerra (Windtalkers, 2002)

O filme é baseado na incrível e verídica história da participação de membros da tribo ameríndia dos Navajos na criação de um código baseado em sua língua, e sua colaboração heróica para a vitória norte-americana sobre os japoneses em 1945. Durante a Segunda Guerra Mundial, ano de 1944, os Estados Unidos levam adiante a guerra contra o Japão, nas ilhas do Pacífico. Mas, algo vai mal para os americanos: o inimigo tem conseguido, de forma inteligente e constante, decifrar todos os códigos utilizados para cifrar as comunicações, e infligido, deste modo, muitas baixas e perdas. Logo é desenvolvido um novo código, este sendo totalmente baseado na desconhecida e complexa língua dos índios Navajos, e, por isto mesmo, perfeito para o objetivo. Para utilizar o novo código são recrutados

dezenas de navajos, que, incorporados às forças armadas, recebem treinamento militar e, principalmente, se tornam aptos a utilizar o código em qualquer situação. (Figura 57)

Figura 57 – Códigos de Guerra

Fonte: http://br.web.img3.acsta.net/medias/nmedia/18/92/28/68/20190522.jpg

O Jogo da Imitação (The Imitation Game, 2014)

Figura 58 – O jogo da imitação

Fonte: http://imagens.publico.pt/imagens.aspx/509298?tp=KM

O filme é uma cinebiografia do criptoanalista inglês Alan Turing, vagamente baseado no livro Alan Turing: The Enigma, de Andrew Hodges. Turing, interpretado por Benedict Cumberbatch, liderou um grupo da inteligência britânica na missão de decifrar os códigos

da máquina Enigma usada pela Alemanha Nazista durante a Segunda Guerra Mundial, sendo um inovador da ciência da computação. Isso ajudou a salvar milhões de vidas, mas depois ele foi condenado por sua homossexualidade. (Figura 58)

Hacker (Blackhat, 2015)

O hacker Hathaway é um gênio da codificação que foi condenado a 15 anos de prisão. Para sair da cadeia antes da conclusão da pena, ele aceita identificar e capturar um hacker que tem feito danos virtuais terríveis com consequências catastróficas no mundo real. (Figura 59)

Figura 59 – Hacker

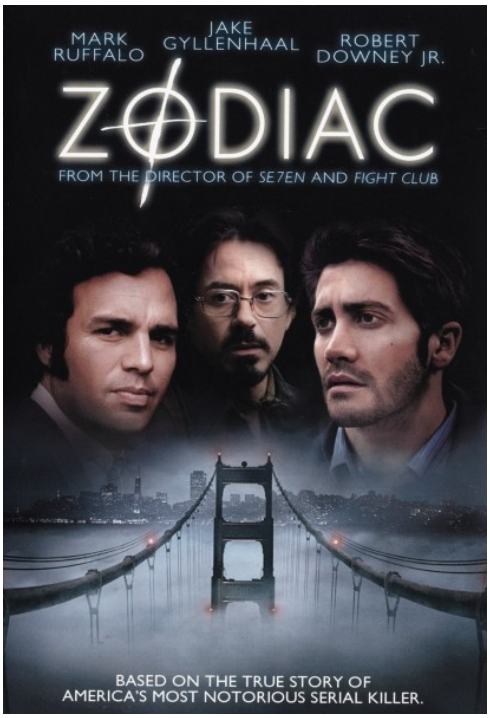
Fonte: http://www.idevicefilmes.com.br/wp-content/uploads/2015/05/Hacker.jpg

Zodíaco (Zodiac, 2007)

1° de agosto de 1969. Três cartas diferentes chegam aos jornais San Francisco Chronicle, San Francisco Examiner e Vallejo Times-Herald, enviadas pelo mesmo remetente. A carta enviada ao Chronicle trazia a confissão de um assassino e as três juntas formavam um código que supostamente revelaria a identidade do criminoso. O assassino exigia que as cartas fossem publicadas, caso contrário mais pessoas morreriam. Um casal de Salinas consegue decodificar a mensagem, mas é Robert Graysmith, um tímido cartunista, quem descobre sua intenção oculta: uma referência ao filme "Zaroff, o Caçador de Vidas"

(1932). Os assassinatos e as cartas se sucedem, provocando pânico na população de San Francisco. (Figura 60)

Figura 60 – Zodíaco



Fonte: http://www.portanova.com.br/filmes/wp-content/uploads/sites/2/2013/02/zodiac-2007-cover-410x600.jpg

O Código da Vinci (The Da Vinci Code, 2006)

Figura 61 – O Código da Vinci

Fonte: https://upload.wikimedia.org/wikipedia/pt/6/6d/Codigo-da-vinci-poster091.jpg

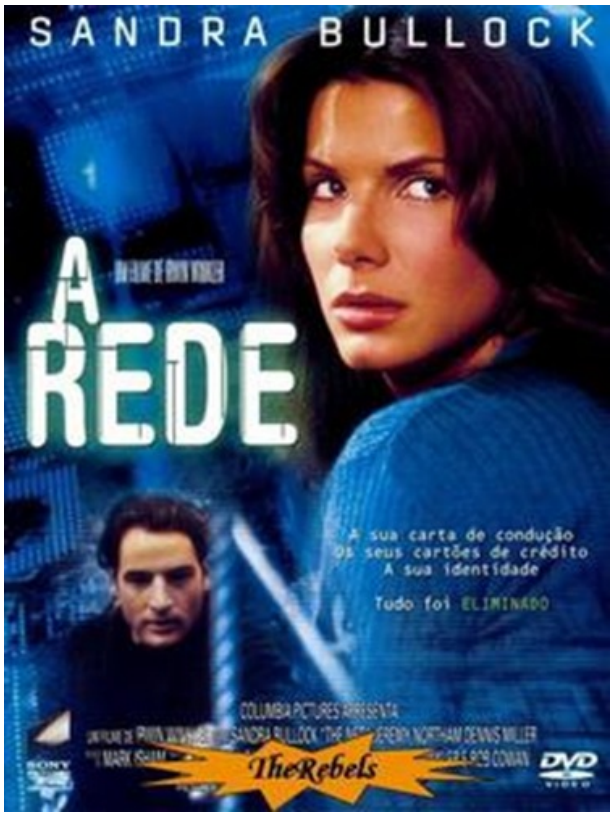
Robert Langdon é um famoso simbologista, que foi convocado a comparecer no Museu do Louvre após o assassinato de um curador. A morte deixou uma série de pistas e símbolos estranhos, os quais Langdon precisa decifrar. Em seu trabalho ele conta com a

ajuda de Sophie Neveu, criptógrafa da polícia. Porém o que Langdon não esperava era que suas investigações o levassem a uma série de mensagens ocultas nas obras de Leonardo Da Vinci, que indicam a existência de uma sociedade secreta que tem por missão guardar um segredo que já dura mais de 2 mil anos. (Figura 61)

A Rede (The Net, 2006)

Hope Cassidy é uma linda especialista em computadores que viaja para Istambul em busca do trabalho perfeito, mas acaba ficando presa em uma enrascada de alta tecnologia. Seus cartões de crédito não funcionam mais, sua conta no banco está vazia e sua identidade foi roubada. Ela começa a ser perseguida quando precisa usar sua inteligência e beleza para recuperar seu nome e também entender o que aconteceu. Com a ajuda de um motorista de táxi e de uma aeromoça, ela vai se deparar com a chocante verdade que a rodeia. (Figura 62)

Figura 62 – A Rede



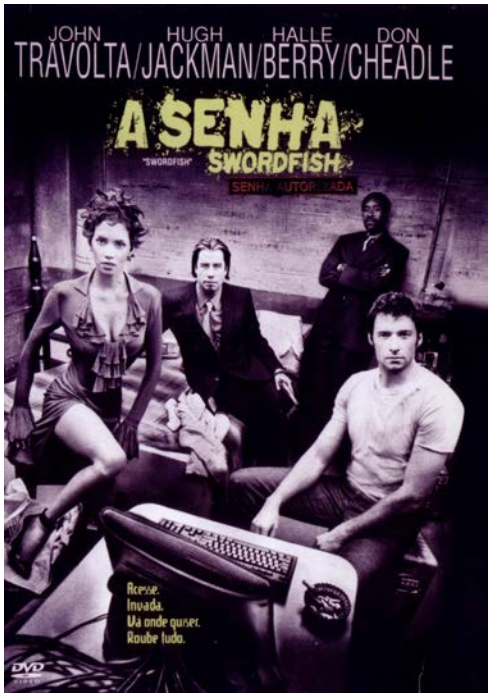
Fonte: http://1.bp.blogspot.com/-ughC8Qxoyhg/VbazaInI2cI/AAAAAAAAQ2A/7OMq-u4l7G0/s640/A-rede-filme-online.jpg

A Senha (Swordfish, 2001)

O mais perigoso espião do planeta tem por missão coagir um hacker que recentemente saiu da prisão a auxiliar no roubo de US 9,5 bilhões de dólares em fundos governamentais. Há um mundo oculto por baixo daquilo que chamamos de ciberespaço, que é protegido por firewalls, senhas e os mais avançados sistemas de segurança. Neste mundo

estão escondidos os maiores segredos, as informações mais incriminadoras e, obviamente, muito dinheiro. (Figura 63)

Figura 63 – A Senha



Fonte: http://br.web.img3.acsta.net/pictures/210/494/21049497_20131014193928221.jpg

Uma Mente Brilhante (A beautiful mind, 2001)

Figura 64 – Uma Mente Brilhante

Fonte: http://www.ccine10.com.br/wp-content/uploads/2013/11/UMA-MENTE-BRILHANTE.jpg

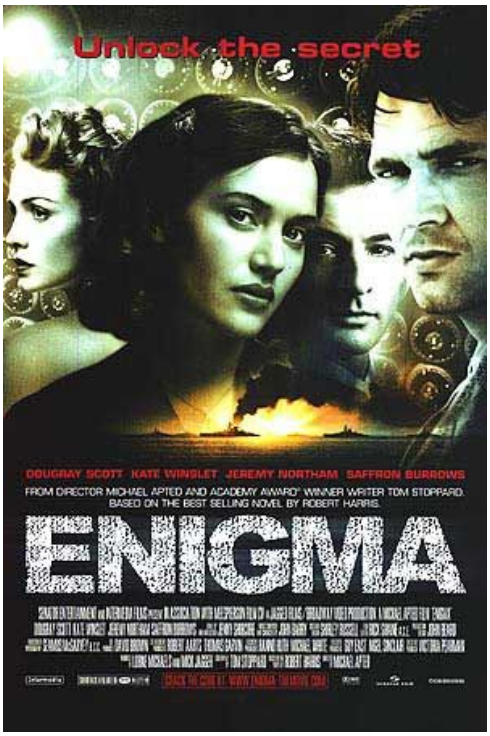
John Nash é um matemático prolífico e de pensamento não convencional, que consegue sucesso em várias áreas da matemática e uma carreira acadêmica respeitável. Após resolver na década de 1950 um problema relacionado à teoria dos jogos, que lhe renderia, em 1994, o Prêmio de Ciências Econômicas em Memória de Alfred Nobel (não

confundir com o Prêmio Nobel), Nash se casa com Alicia. Após ser chamado a fazer um trabalho em criptografia para o Governo dos Estados Unidos, Nash passa a ser atormentado por delírios e alucinações. Diagnosticado como esquizofrênico, e após várias internações, ele precisará usar de toda a sua racionalidade para distinguir o real do imaginário e voltar a ter uma vida normal assim como seus amigos. (Figura 64)

Enigma (2001)

Em março de 1943, a equipe de elite dos decodificadores da Inglaterra tem uma responsabilidade monumental: decifrar o Enigma, um código ultraseguro utilizado pelos nazistas para enviar mensagens aos seus submarinos. O desafio fica ainda maior quando se sabe que uma grande esquadra de navios mercantis está prestes a cruzar o Atlântico e cerca de dez mil homens correrão perigo caso a localização dos submarinos alemães não seja logo descoberta, o que apenas poderá ocorrer quando o Enigma for decifrado. Para liderar este trabalho é chamado Tom Jericho, um gênio da matemática que consegue realizar tarefas consideradas impossíveis pelos especialistas. Porém, ao mesmo tempo em que Jericho se envolve cada vez mais com a decodificação do Enigma ele precisa estar atento à sua namorada Claire, uma sedutora e misteriosa mulher que pode estar trabalhando como espiã para os alemães. (Figura 65)

Figura 65 – Enigma



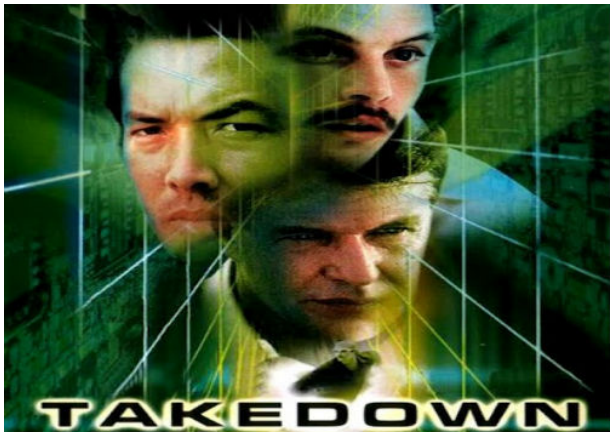
Fonte: https://upload.wikimedia.org/wikipedia/en/e/e1/Enigma_film.jpg

Hackers 2 – Caçada Virtual (Takedown, 2000)

Kevin Mitnick, habilidoso hacker, consegue acesso aos arquivos do FBI, tornando-se um dos piratas de informática mais procurados dos EUA. Para capturá-lo, o agente McCoy

Rollins conta com a ajuda de Tsutomo Shimomura, gênio da informática responsável por traçar as pistas deixadas por Kevin no ciberespaço. (Figura 66)

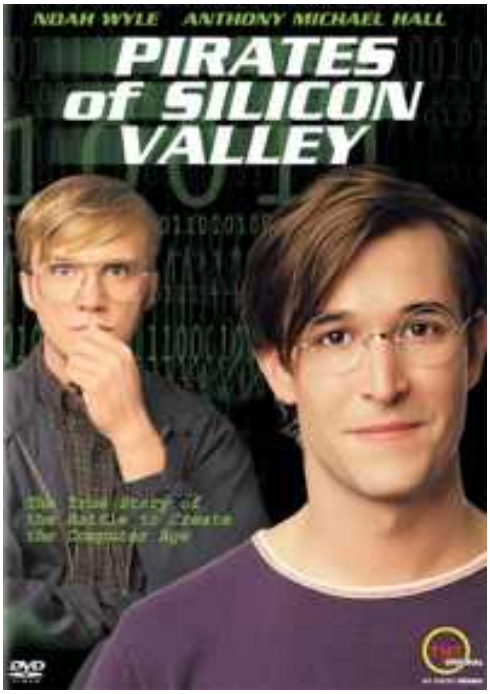
Figura 66 – Takedown



Fonte: https://petcivilufjf.files.wordpress.com/2013/04/operation-takeodown.jpg

Piratas do vale do silício (Pirates of Silicon Valley, 1999)

Figura 67 – Piratas do Vale do Silício



Fonte: http://www.static-yesfilmes.org/imagens/2606d7f3be.jpg

O filme conta através das personalidades de Steve Jobs, Steve Wozniak, Bill Gates, entre outros, o desenvolvimento da história da microinformática e da popularização dos computadores. Mostra algo sobre a luta de alguns estudantes contra o domínio da produção de computadores por grandes empresas e também faz uma abordagem a cerca das primeiras reações culturais a esse processo de popularização. Embora não houvesse

computadores pessoais como os que tão comumente encontramos hoje, existia um público ansioso por poder usufruir dessa tecnologia. (Figura 67)

Código para o inferno (Mercury Rising, 1998)

Quando uma operação não tem o resultado esperado Arthur Jeffries, um agente do F.B.I., se torna bode expiatório e é relegado a segundo plano, sendo usado só em operações de rotina. Mas sua vida tem uma radical mudança quando Simon Lynch, um menino de nove anos autista, sem o menor esforço desvenda um "indecifrável" código do governo americano que tinha custado dois bilhões de dólares. Assim, o responsável pelo projeto ordena que este contratempo em forma de criança seja eliminado, mas o agente encarregado da missão mata os pais do garoto (e simula que o marido matou a mulher e se suicidou), mas a criança não é encontrada. Jeffries descobre Simon em um esconderijo e não aceita a versão do "suicídio". Fica claro que querem o garoto morto, ele não sabe quem e nem o motivo mas decidiu protegê-lo e sozinho, pois não sabe em quem confiar. (Figura 68)

Figura 68 – Código para o Inferno

Fonte: http://telecine.img.estaticos.tv.br/cache/cartazes/codigo-para-o-inferno_cartaz_220x283.jpg

Quebra de Sigilo (Sneakers, 1992)

Dezembro de 1969. Cosmo e Martin são hackers, que se divertem transferindo grandes somas de contas de pessoas conservadoras para grupos no mínimo contestadores. A polícia fica sabendo o que eles estavam fazendo e vai prendê-los, mas Martin consegue escapar pois tinha ido comprar uma pizza. Décadas depois, Martin Bishop (cujo verdadeiro nome é Brice) lidera um grupo de hackers do qual fazem parte: Donald Crease, um ex-agente da CIA; Erwin "Assobio" Emory, que, apesar de ser cego, enxerga muita coisa que os outros não enxergam; Darryl "Mamãe" Roskow, que já esteve preso; e Carl Arbegast,

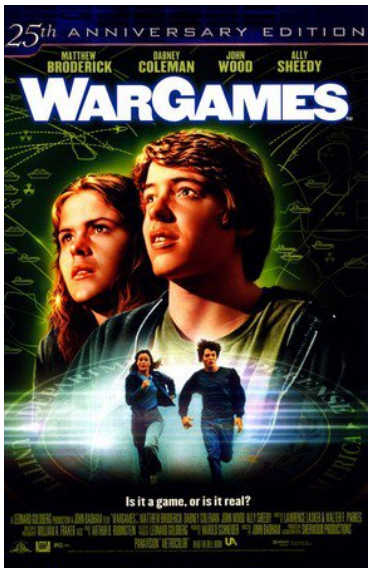
um jovem gênio em computação. Eles são pagos para "assaltarem" bancos, mas quem os contrata na verdade são os donos dos bancos, pois querem que Martin relate as falhas na segurança. (Figura 69)

Figura 69 – Quebra de Sigilo

Fonte:
http://www.blogdafei.com.br/wp-content/uploads/2015/11/Assistir-Quebra-de-Sigilo-Dublado-Online.jpg

Jogos de guerra (WarGames, 1983)

Figura 70 – Jogos de Guerra



Fonte:
https://cdn.fstatic.com/media/movies/covers/2012/10/thumbs/9fd3eea49a8ec62e3ff247067c75ed2d_jpg_290x478_upscale_c

O hacker David Lightman pode entrar nos mais avançados sistemas de segurança, desvendar o código secreto mais intrincado e vencer os jogos de computador mais avançados. Mas, quando ele acidentalmente entra no computador de guerra do Departamento de Defesa, ele inicia um confronto de proporções mundiais – a 3ª Guerra Mundial. Com sua colega e um mago da computação, David tem que correr contra o tempo para vencer seu oponente e impedir um Armagedom nuclear. (Figura 70)

LIVROS

O Código Da Vinci de Dan Brown (2003)

A maioria dos quebra-cabeças que são resolvidos por personagens no romance não são cifras por natureza, já que sugerem que não há nenhuma solução única e se baseiam na intuição, o conhecimento e/ou a imaginação dos personagens. No entanto, o livro oferece vários exemplos de sistemas de cifras históricas reais, o mais notável é a cifra Atbash. Como você deve ter adivinhado, esta cifra não oferece nenhum desafio para a criptoanálise, pois representa o mesmo princípio do cifrado de substituição simples. No entanto, esta cifra pode tornar-se relativamente confiável se uma análise de frequência torna-se impossível depois de transmitir um texto curto. No entanto, a heroína principal da história, uma criptógrafa da polícia francesa, mantém um certo orgulho em estar familiarizada com os sistema de cifra. (Figura 71)

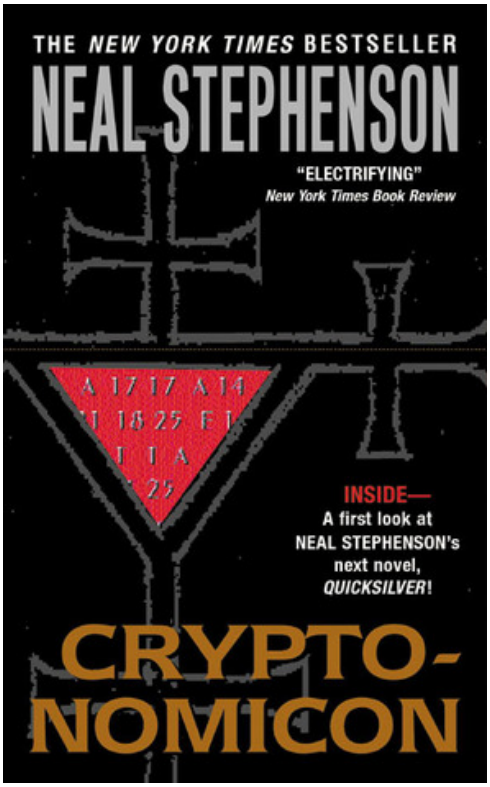
Figura 71 – O Código Da Vinci

Fonte: https://upload.wikimedia.org/wikipedia/pt/thumb/6/6b/DaVinciCode.jpg/200px-DaVinciCode.jpg

Cryptonomicon por Neal Stephenson (1999)

Supondo que Edgar Allen Poe descobriu a criptografia nas obras literárias, Neal Stephenson levou-a para o próximo nível. A base do Cryptonomicon são essencialmente as cifras e tudo aquilo relacionado ao tema. O enredo do período ocorre na Segunda Guerra Mundial e é dedicada ao confronto de criptógrafos e o conflito que atravessaram (incluindo quebrar o código Enigma e as consequências produzidas). Os personagens da segunda linha do enredo, que se desenvolve durante a bolha das pontocom, criaram algo que nos faz recordar o Bitcoin. Stephenson não se coíbe em dedicar várias páginas para elucidação de princípios matemáticos ou físicos necessários para a compreensão de como tudo funciona. A obsessão de Stephenson com a criptografia atinge sua apoteose no apêndice do livro, que contém uma descrição completa do sistema de criptografia que foi usado por um de seus personagens. A cifra utiliza um baralho de cartas, embaralhados em uma determinada ordem, como uma chave. O apêndice tem um manual completo sobre como usar a cifra, criar a chave, e sobre as precauções para aqueles que decidirem aplicar o método na vida real. (Figura 72)

Figura 72 – Cryptonomicon



Fonte: http://d.gr-assets.com/books/1327931476l/816.jpg

Fortaleza Digital de Dan Brown (1998)

Ensei Tankado, um ex-funcionário da Agência de Segurança Nacional (NSA) que jura vingar-se dos Estados Unidos, desenvolve um algoritmo de encriptação inquebrável, algo considerado impossível, que caso seja publicamente utilizado inutilizará o computador

superpotente da NSA, TRANSLTR, na decodificação de mensagens. A este algoritmo dá o nome de Fortaleza Digital. (Figura 73)

Figura 73 – Fortaleza Digital

Fonte:http://isuba1-a.akamaihd.net/produtos/01/00/item/6625/4/6625450_1GG.jpg

As aventuras de Sherlock Holmes - Volume IV - Os Dançarinos por Arthur Conan Doyle (1903)

Figura 74 – Os Dançarinos

Fonte:http://static.wmobjects.com.br/imgres/arquivos/ids/2928088-344-344/os-dancarinos—col–sherlock-holmes.jpg

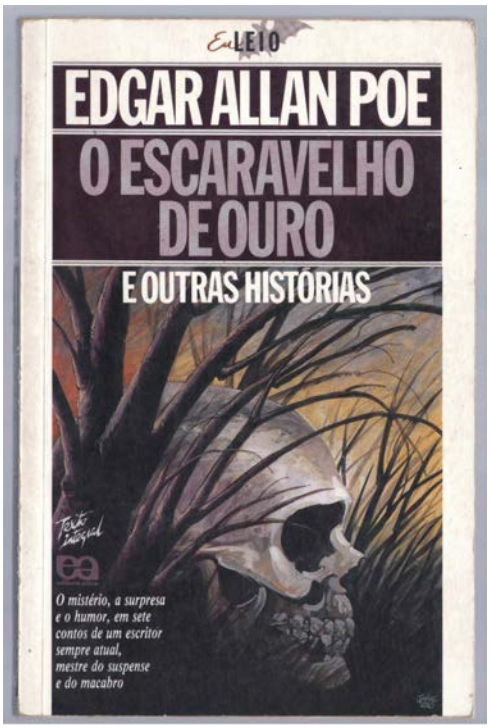
Neste livro, no conto Os Dançarinos, Doyle envolveu seu famoso personagem Sherlock Holmes numa trama criptográfica. Pequenos homenzinhos dançantes começam a aparecer desenhados ao redor da propriedade do Sr. Curbitt. Parecem desenhos de criança e ele não daria grande importância a eles não fosse a estranha reação de sua esposa. Casado há um ano, o Sr. Curbitt apenas sabe que sua mulher veio da América, desconhecendo detalhes de sua história pregressa. Temendo o significado dos intrigantes desenhos que não param de aparecer e atemorizar sua esposa, Curbitt procura Sherlock

Holmes. Para solucionar o caso, o detetive tem que decifrar esse código em que figuras em diferentes poses de dança substituem as letras. (Figura 74)

O Escaravelho de Ouro por Edgar Allan Poe (1843)

A história completa do Escaravelho Dourado é uma narrativa em primeira pessoa da leitura de um documento cifrado e da resolução de um enigma que revela ao Capitão Kidd os tesouros. O texto cifrado é representado por um conjunto aleatório de números e símbolos, e a história revela minuciosamente o caminho dos pensamentos do protagonista, que escolheu para analisar a frequência de aparecimento de símbolos e letras no idioma Inglês. Ao substituir cada letra, ele apresenta e refuta a hipóteses sobre possíveis sobreposições baseadas em combinações frequentes das letras neste idioma. Mesmo em 1843, quando a história foi escrita, a cifra de substituição não foi considerada algo extraordinário. No entanto, foi um dos primeiros relatos populares de um sistema criptográfico e, por este motivo, atraiu muita atenção. Depois que a história foi publicada, houve um concurso em um jornal onde Poe resolveu cifras enviadas pelos leitores do jornal. (Figura 75)

Figura 75 – O Escaravelho de Ouro



Fonte:http://mlb-s2-p.mlstatic.com/o-escaravelho-de-ouro-e-outras-historias-edgar-allan-poe-13995-MLB185410953_1872-F.jpg

Fontes:

http://www.sbmac.org.br/eventos/cnmac/xxxi_cnmac/PDF/189.pdf

https://mundosherlock.wordpress.com/canon_e/arthur-conan-doyle-a-volta-de-sherlock-holmes-1905/os-dancarinos/

https://blog.kaspersky.com.br/best-fiction-with-ciphers-explanation/5382/

APÊNDICE D

Códigos

Algumas pessoas usam as palavras código e cifra com significados equivalentes, mas são duas coisas diferentes. Um código secreto é um sistema no qual toda palavra ou frase da sua mensagem é trocada por outra palavra, frase ou símbolos, alterando o sentido da mensagem. Uma cifra é um sistema onde cada letra da sua mensagem é substituída por outra letra ou símbolo. A cifra envolve uma chave criptográfica, enquanto o código não. Os códigos podem ser usados em conjunto com as cifras para que a mensagem fique ainda mais difícil de ser decifrada.

Por exemplo, "A águia está sobrevoando o ninho" pode ser um código para avisar que alguém está chegando. Claro que quem vai receber a mensagem deve estar a par das palavras e seus respectivos códigos, logo devem haver um livro de códigos com o emissor e outro com o receptor da mensagem.

Um código famoso por sua utilização na Segunda Guerra Mundial entrou para o cinema no filme Códigos de Guerra. Durante a Segunda Guerra, os americanos recrutaram 420 índios Navajos para transmitir dados criptografados usando palavras de seu idioma. A letra "a", por exemplo, era cifrada por "wol-la-chee", que quer dizer "formiga" em Navajo (ou "ant"em inglês). Com esse código totalmente baseado na desconhecida e complexa língua dos índios Navajos e com sua participação heroica na guerra, os Estados Unidos conquistaram a vitória sobre os japoneses em 1945.

São muitos tipos de códigos utilizados desde o passado até os dias de hoje. Escolhi o código de barras e o código Morse para dar uma atenção especial, com o propósito de enriquecer ainda mais esse trabalho. O código de barras foi escolhido pela sua importância para a sociedade nos dias de hoje e o código Morse pela sua importância histórica.

D.1 Código de barras

Disponível em http://mundoestranho.abril.com.br/materia/como-funciona-o-codigo-de-barras

Figura 76 – Código de Barras

Fonte: http://www.proteste.org.br/site_images/articles/codigo.jpg

O código de barras nada mais é do que a representação gráfica da sequência de algarismos que vem impressa logo abaixo dele. A vantagem das barras é que elas podem ser identificadas rapidamente, e sem risco de erros, por aparelhos portáteis de leitura óptica, como os usados pelos caixas de supermercado. Mas o que realmente importa para identificar o produto é sua sequência numérica, que também pode ser digitada manualmente pelos caixas. "Esse número funciona como uma espécie de RG do produto, ou seja, não existem dois produtos diferentes com o mesmo número", diz a desenhista industrial Cláudia Ferreira, consultora da EAN, organização internacional que gerencia a distribuição dos códigos no mundo e tem uma representação no Brasil. O sistema de barras foi criado nos Estados Unidos em 1973 e acabou sendo adotado na Europa três anos depois. Mas, enquanto os americanos usam uma sequência numérica de 12 dígitos, os europeus optaram por um padrão com 13, que foi adotado no resto do mundo.

A partir de 2005, porém, os dois sistemas foram unificados. Mas isso não significa que toda a confusão numérica acabou, pois existem ainda outros tipos de códigos especiais, como o formado por 14 dígitos (usado em caixas de papelão para informar a quantidade de produtos guardados) e o de oito dígitos (utilizado quando a embalagem do produto é muito pequena).

Linguagem cifrada *Sistema mais comum, desenvolvido na Europa, usa 13 algarismos para cada produto*

As barras são uma representação gráfica do código binário. Cada traço preto ou branco equivale a um bit (1 ou 0, respectivamente) e cada algarismo é sempre representado por sete bits. Uma barra escura mais grossa que as outras é, na verdade, a somatória de vários traços pretos. O mesmo princípio vale para as barras brancas.

AVISO INICIAL

As três primeiras barras mais compridas (uma branca no meio de duas pretas) são uma sinalização, indicando que a seguir vem o código do produto. As barras e seus respectivos algarismos não ficam alinhados - por isso o número 7 vem antes das barras de sinalização.

REGISTRO NACIONAL

Esses três primeiros números (789) indicam que o produto foi cadastrado no Brasil, apesar de não necessariamente ter sido fabricado aqui. Cada país tem uma combinação própria. A da Argentina, por exemplo, é 779.

RG DO FABRICANTE

A segunda sequência de números, que pode variar de quatro a sete algarismos, é a identificação da empresa fabricante. Esse número é fornecido por uma organização internacional, a EAN, que faz o controle para que não sejam distribuídos números iguais.

RG DO PRODUTO

A terceira sequência identifica o produto em si. A numeração varia conforme o tipo, o tamanho, a quantidade, o peso e a embalagem do produto - uma Coca-Cola em lata, por exemplo, tem uma sequência diferente de uma em garrafa.

CHECAGEM FINAL

O último número é um dígito verificador. Ao ler todo o código do produto, o computador faz um cálculo complexo, somando, dividindo e multiplicando os dígitos anteriores. Se a leitura estiver correta, o resultado desse cálculo estranho é igual ao do dígito verificador.

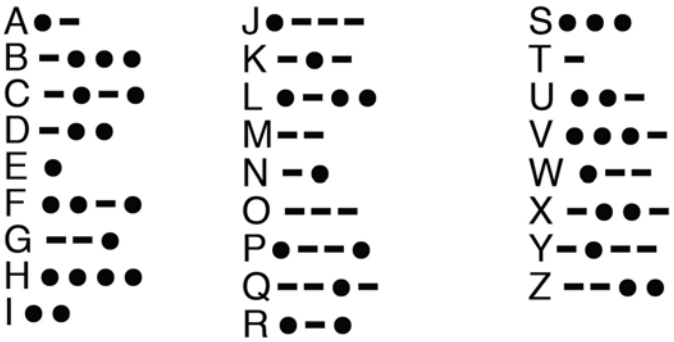
D.2 Código Morse

Disponível em http://www.infoescola.com/comunicacao/codigo-morse/

O código Morse é um método de transmissão de uma informação em texto, com o uso de dois tons sonoros distintos, que podem apenas ser compreendidos por um ouvinte habilitado. O código Morse Internacional abarca o alfabeto latino convencional, algumas outras letras romanas, e os números arábicos, além de uma pequena quantidade de pontuação e sinais padrões, tudo sendo de possível codificação usando apenas pontos, traços e espaços. Como diversas línguas possuem alfabetos próprios, várias extensões foram aplicadas ao código Morse convencional, possibilitando o seu uso em diversos idiomas.

Cada caractere (letra ou número) é representado por uma sequência única de pontos e traços. A duração de um traço é equivalente ao triplo do tempo de um ponto. Cada ponto ou traço é seguido de um curto silêncio, igual à duração de um ponto. As letras de uma palavra são separadas por um espaço, igual a três pontos, e uma palavra é separada da

Figura 77 – Código Morse



Fonte: http://www.infoescola.com/wp-content/uploads/2013/02/codigo-morse.jpg

outra por um espaço de sete pontos. A duração do ponto é a unidade de medida básica na medição do tempo em transmissões codificadas. A duração de cada caractere em Morse é de aproximadamente inversamente proporcional à sua frequência da sua ocorrência no idioma inglês. Assim, a letra mais comum em inglês, a letra "E", tem o código mais curto, um único ponto.

O código Morse é a forma codificada de comunicação mais popular entre os radioamadores. Hoje, o Morse não é mais necessário para que alguém se forme como operador de rádio. Pilotos e controladores de tráfego aéreo, por exemplo, apenas precisam de um entendimento geral para se formarem. Dados de dispositivos auxiliares na navegação aeronáutica, como VOR e radiofarol, são constantemente apresentados em Morse. Comparado à transmissão em voz, o Morse é menos sensível à condições climáticas, além de ser capaz de ser decodificado sem a necessidade de um dispositivo especial. O código Morse é uma alternativa útil para o envio de dados para ouvintes em canais de voz, pois muitos repetidores de rádio amador, por exemplo, são capazes de transmiti-lo, mesmo que eles sejam utilizados para comunicações de voz.

Para sinais de emergência, o código Morse pode ser enviado com o uso de equipamentos improvisados, tornando-o um dos métodos mais versáteis de telecomunicação. O sinal de socorro mais comum é o SOS, formado por três pontos, três traços e três pontos. Esse sinal é internacionalmente reconhecido.

A origem do código Morse remonta a criação do sistema de telégrafo elétrico, desenvolvido no começo de 1836, pelo artista Samuel Morse, o físico Joseph Henry e o inventor Alfred Vail, todos americanos. Esse sistema, enviava pulsos elétricos através de cabos conduzidos por um eletroímã, posicionado no local receptor. Obviamente, um código teria de ser criado para a transmissão de uma linguagem, usando apenas esses três pulsos elétricos, além do espaço entre eles. Samuel Morse, portanto, criou e desenvolveu aquilo que seria o precursor do Código Morse Internacional, usado hoje.

Em 1837, William Cooke e Charles Wheatstone, na Inglaterra, começaram a usar um telégrafo elétrico que também usava eletroímãs em seus receptores. No entanto, diferente de qualquer outro sistema linguístico formado por cliques, eles usavam um sistema de agulhas que giravam acima de alfabetos para indicar as letras que estavam sendo enviados. Em 1841, Cooke e Wheatstone construíram um telégrafo que imprimia as letras em uma roda de tipos. Esta máquina foi baseada em seu telégrafo de 1840 e funcionou bem. No entanto, eles não conseguiram encontrar clientes para este sistema, e apenas dois exemplares foram já construídos.

Por outro lado, o sistema telegráfico dos três americanos, inaugurado em 1844, foi projetado para fazer registros em uma fita de papel quando correntes elétricas fossem recebidas. O receptor original do telégrafo Morse utilizava um mecanismo de rodas mecânicas para mover a fita. Quando uma corrente elétrica era recebida, um eletroímã acionava uma caneta na fita de papel, que estaria em movimento, fazendo um recorte na fita. Quando a corrente era interrompida, a caneta era retraída, para que a porção da fita que não tivesse sido utilizada continuasse sem marcas.

O código Morse foi desenvolvido para que os operadores pudessem decodificar as marcas deixadas na fita de papel em mensagens inteligíveis. Em seu primeiro sistema, Morse planejava transmitir somente números, e usar um dicionário para que o receptor procurasse cada palavra de acordo com o número que tinha sido enviado. No entanto, o código logo foi expandido por Alfred Vail, recebendo letras e caracteres especiais, para que pudesse ser utilizado de modo mais abrangente. Vail determinou a frequência de uso das letras no idioma Inglês, às letras mais usadas foram atribuídas as sequências mais curtas de pontos e traços, às menos usadas foram atribuídas as sequências mais longas. Logo, os operadores perceberam que podiam perfeitamente ouvir os pontos e traços emitidos pelos pulsos elétricos, escrevendo a mensagem numa folha de papel, descartando, assim, o uso da fita de papel operada mecanicamente.

Quando o código Morse foi adaptado para comunicação por rádio, os pontos e traços passaram a ser enviados na forma de pulsos curtos e longos, respectivamente. Percebeu-se, mais tarde, que as pessoas se tornavam mais eficiente em lidar com o código Morse quando ele lhes era ensinado como uma linguagem sonora.

Na década de 1890, o código Morse começou a ser usado extensivamente no início das comunicações em rádio, antes de ser possível transmitir voz. No século XIX e início do século XX, a maioria das comunicações em alta velocidade de comunicação utilizavam o código Morse através dos telégrafos, cabos submarinos e alguns circuitos de rádio. Na aviação, o código Morse por rádio começou a ser usado regularmente nos anos de 1920. As aeronaves levavam, em sua tripulação, um indivíduo capaz de decodificar e enviar mensagens, por código Morse, para as estações em terra.

A partir dos anos 1930, ambos os pilotos civis e militares foram obrigados a se

especializarem em código Morse, pois os sistemas de comunicação e identificação de pontos de navegação eram transmitidos através de mensagens contínuas levando dois ou três letras codificadas em código Morse.

A radiotelegrafia, usando o código Morse, foi de fundamental importância durante a Segunda Guerra Mundial, especialmente na transmissão de mensagens entre os navios de guerra e as bases navais de diversos países envolvidos no conflito. As comunicações de longo alcance entre navios eram feitos por radiotelegrafia, usando mensagens criptografadas, porque os sistemas de rádio por voz ainda eram muito limitados, tanto em alcance quanto segurança. Esse mecanismo também foi bastante usado por aviões de guerra, especialmente os patrulheiros, que enviavam para os seus comandos a posição de navios, tropas e aeronaves inimigas. As estratégias de batalha em terra também mudaram muito graças à radiotelegrafia. As ofensivas blitzkrieg alemãs, por exemplo jamais seriam realizadas se uma extensa rede de comunicação rápida não estivesse dando apoio às tropas.

O código Morse foi usado como uma comunicação marítima padrão até 1999, quando foi substituído pelo Sistema Mundial de Socorro e Segurança Marítima. Quando a Marinha Francesa cessou o uso do Código Morse, a 31 de Janeiro de 1997, a mensagem final transmitida foi: "Chamando todos. Esse é o nosso último brado antes do silêncio eterno". Hoje, quase nenhuma nação, oficialmente, monitora transmissões em código Morse.

APÊNDICE E

Números primos e a Criptografia RSA

No primeiro capítulo falamos um pouco da história da criptografia, desde de sua origem até a criptografia RSA. A proposta desde capítulo é explicar como funciona esse sistema.

Já sabemos que no final da década de 70, Ron Rivest, Adi Shamir e Leonard Adleman revolucionaram a Criptografia criando um padrão de codificação de dados, o RSA, fácil de fazer e difícil de desfazer. A popularidade do RSA se baseia na existência de duas chaves, uma pública (um padrão de codificação para envio de mensagens) e uma privada (o instrumento de decodificação). O remetente da mensagem conhece as chaves públicas dos seus amigos. Elas são cadeados personalizados que qualquer um pode fechar, mas só um sabe abrir. Escrita a mensagem, o remetente usa o cadeado para criptografá-la. Ele “tranca” o conteúdo e se certifica de que só o destinatário será capaz de lê-lo. Com a chave privada, que só ele possui, o destinatário abre o cadeado e assim decifra os dados enviados. É ela que garante a segurança da operação.

A criptografia RSA é muito segura e é a matemática que garante isso. O RSA faz uso dos números primos e da operação de fatoração para garantir essa segurança.

Para entendermos como ela funciona primeiro vamos relembrar alguns conceitos importantes já estudados na dissertação de LOUREIRO (2014, p.26-29):

Definição 6 *Chamamos de números primos, números naturais maiores que* 1*, divisíveis apenas por* 1 *e por ele mesmo.*

Os primeiros números primos são: $2, 3, 5, 7, 11, 13, \cdots$. Dois importantes resultados envolvendo números primos são: o teorema fundamental da aritmética e a infinitude dos números primos. Vamos fazer aqui a demonstração desses dois resultados.

Para demonstrarmos o Teorema Fundamental da Aritmética é necessário o seguinte resultado.

Lema 1 *Todo número inteiro* $a \geq 2$ *possui pelo menos um divisor primo*

Teorema 3 (Fundamental da Aritmética) *Todo número natural pode ser decomposto em fatores primos de maneira única.*

Demonstração 1 *Dado um número inteiro n, vamos mostrar por indução que $n = p_1 \cdot p_2 \cdots p_r$, com cada p_j sendo um número primo.*

De fato, para $n = 2$ o teorema é válido.

Se $n > 2$ e n for primo, o teorema também é válido pois basta tomarmos $p_1 = n$.

Considere então que $n > 2$ é composto, e que a hipótese de indução é que todo número menor que n admite decomposição em fatores primos. Por causa do lema anterior, existe um número primo p_1 tal que p_1 divide n, ou seja, existe um $q \in \mathbf{Z}$ tal que $n = p_1 q$. Se q for primo então o resultado está provado, mas se q for composto então pelo princípio de indução existem números primos tais que q é o produto desses primos. Portanto n é a junção dos fatores primos de q com p_1.

Vamos demonstrar agora a unicidade do teorema.

Suponhamos que

$$n = p_1 p_2 p_3 \cdots p_r e n = q_1 q_2 q_3 \cdots q_s$$

Com p_i, q_j primos maiores que $0 e 1 \leq i \leq r$, $1 \leq j \leq s$. Como p_1 divide $q_1 q_2 q_3 \cdots q_s$ então p_1 divide q_i para algum i. Sem perda de generalidade podemos supor $i = 1$. Daí p_1 divide q_1 e como ambos são primos, logo $p_1 = q_1$. Com isso temos que

$$p_1 p_2 p_3 \cdots p_r = p_1 q_2 q_3 \cdots q_s$$

Como $p_1 \neq 0$, simplificando, obtemos $p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$. Repetindo este processo, chegaremos que $r = s$ e após um rearranjo dos índices q_j, encontramos $p_1 = q_1$, $p_2 = q_2$, $p_3 = q_3$, $p_r = q_r$.

Teorema 4 *Existem infinitos números primos*

Demonstração 2 *Suponha por absurdo que existem n números primos, denotados por p_1, p_2, $\cdots$, p_n, tais que $p_1 < p_2 < p_3 \cdots < p_n$. Considere o número natural $x = (p_1 \cdot p_2 \cdots p_n) + 1$. O número x não é divisível por nenhum dos números p_1, p_2, $\cdots$, p_n pois sempre deixa resto 1. Esse resultado contradiz o teorema fundamental da aritmética citado acima, logo existem infinitos números primos.*

Neste momento apresentaremos em linhas gerais como funciona o RSA e explicar porque ele é difícil de ser decifrado. O funcionamento preciso do RSA requer muitas ferramentas matemáticas, mas podemos entender como se dá o seu funcionamento, pois sua base está montada em cima da dificuldade de se decompor um número em fatores primos.

O RSA faz uso dois números primos que vamos chamar de p e q. Para codificar uma mensagem usando o RSA é suficiente conhecermos o produto desses dois primos, que vamos chamar de N, isto é, $N = p.q$. Já para decifrar a mensagem, precisamos conhecer os valores de p e q. A chave de codificação do RSA é portando, constituída essencialmente pelo número N. Essa chave é tornada pública. Já a chave de decodificação é constituída pelos números primos p e q. Essa é a chave secreta que deve ser mantida em segredo, pois quem souber o valor de p e q poderá decifrar a mensagem. (COUTINHO, 2000)

Digamos que Bob queira enviar uma mensagem para Alice. Então, Bob verifica com Alice, qual é a sua chave pública e Alice informa o valor N, mas em hipótese alguma deve revelar quais números primos ela usou para formar N. De posse do valor N, Bob cifra a mensagem usando N como chave cifradora e envia a mensagem cifrada para Alice. Ao receber o texto cifrado, Alice utiliza os números primos p e q que formaram o número composto N para decifrar o texto. Pode-se imaginar que é fácil quebrar o RSA, basta fatorar N que obteremos a chave secreta p e q. Isto está correto. Digamos que, uma pessoa mal intencionada, Eva, esteja ouvindo a conversa entre Bob e Alice. Eva irá ouvir Alice informando a Bob a chave N e sabendo que irá ser cifrada usando o RSA, esta deverá apenas decompor o valor de N para obter a chave secreta p e q e assim conseguirá ler a mensagem. Decifrar um texto cifrado pelo RSA teoricamente é fácil, basta usar a fatoração. O desafio é que não existe nenhum algoritmo prático de fatoração. Para se ter uma ideia de como o processo de decomposição é extremamente trabalhoso, COUTINHO (2000) relata que pouco depois do RSA ser inventado, uma mensagem desafio foi codificada usando uma chave pública de 129 algarismos, que ficou conhecida como RSA-129. Em 1994, 17 anos depois e com o uso de 600 computadores espalhados por 25 países e um supercomputador foi possível fatorar a chave e decifrar a mensagem. Veja que o RSA-129 foi proposto na década de 80. Se para quebrar uma chave pública de 129 algarismos demorou-se todo esse tempo, imagina então decompor números com milhares de casas decimais. Essas são as chaves públicas usadas atualmente. Veja que, conhecer a chave cifradora não te permite descobrir a chave secreta.

A tarefa de se decompor números primos ainda é um desafio. Tanto que até o ano de 2007, o site oficial do RSA propunha desafios com prêmios em dinheiro para quem conseguisse decompor certos números. Os prêmios foram cancelados, mas os desafios ainda existem e poucos foram resolvidos.

Anexos

ANEXO A

Texto da Atividade 1

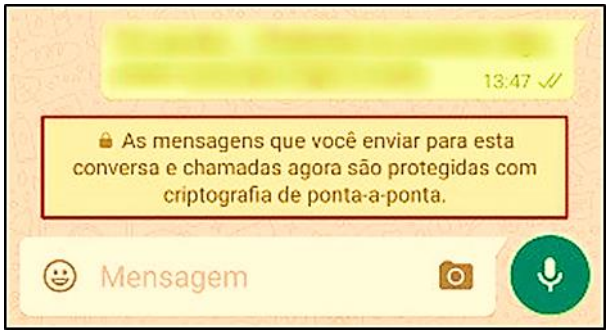
Hikari em: CRIPTOGRAFIA??

Você já viu essa mensagem no seu Whatsapp?

Você conhece ou já tinha ouvido falar na palavra **criptografia?**

Sabe o que significa?

E "criptogragia de ponta-a-ponta", o que será?



Na primeira semana de abril, o WhatsApp começou a notificar os usuários do aplicativo de que já está utilizando a chamada criptografia de ponta-a-ponta, mas o que seria isso? Antes de qualquer coisa, precisamos entender o que é criptografia.

A palavra criptografia é de origem grega, cripto (do grego kryptos) significa ocultar e grafia (do grego graphein) significa escrever, então criptografia seria a escrita oculta ou escrita secreta. Seu estudo está ligado à necessidade de se guardar ou transferir informações com segurança. A criptografia faz parte da ciência chamada de Criptologia, e faz uso da Matemática para construir sistemas criptográficos cada vez mais seguros. Chamados também de algoritmos, cifras, códigos, os sistemas criptográficos transformam uma mensagem clara em uma mensagem ilegível.

A criptografia de ponta-a-ponta é um recurso de segurança utilizado pelos administradores do aplicativo Whatsapp. O sistema visou criptografar (cifrar a mensagem para que seja impossível ser lida quando armazenada) nas duas "pontas" da mensagem (pessoas que estão conversando). Ela assegura que somente você e a pessoa com que você está se comunicando podem ler o que é enviado e ninguém mais. As suas mensagens estão seguras com um "cadeado" (um sistema criptográfico) e somente o emissor (quem envia) e o receptor (quem recebe) possuem a "chave secreta" (tipo uma senha) necessária para destrancá-lo e ler a mensagem.

Nada muda para quem usa o programa. A vantagem desse tipo de criptografia é que o processo é invisível e não exige nenhuma ação por parte dos usuários. As chaves são recebidas e utilizadas automaticamente.

As conversas criptografadas trafegam de maneira "embaralhada" pela internet, de tal maneira que nem mesmo um grampo policial é capaz de enxergar o conteúdo do bate-papo e dos arquivos que são transferidos. Uma conversa protegida não pode ser desembaralhada nem mesmo pelos hackers (profissionais da computação), ou crackers (criminosos da internet) e nem mesmo pelo próprio WhatsApp.

Então, gostou de saber um pouco mais?

Tchau e até a próxima!

ANEXO B

Texto da Atividade 2

Hikari em:

ATRPNSIOSOCA

A criptografia está muito avançada atualmente. Sistemas criptográficos cada vez mais complexos são criados. O avanço da computação tornou possível e também necessário. Possível porque, com a evolução dos computares, métodos mais eficientes de criptografia se tornaram viáveis. E, necessário porque a troca de informação à distância, via internet, precisava se tornar segura. Porém nem sempre foi assim, ao longo da História existiram muitos fatos curiosos ligados à Criptografia.

No século V a.C., os gregos antigos, e em particular os espartanos, utilizavam uma forma curiosa para se comunicar durante as batalhas militares.

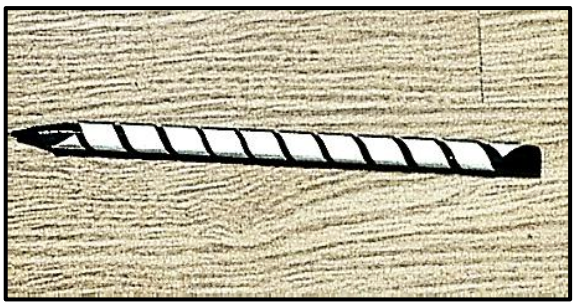
Os espartanos tinham um bastão de madeira, conhecido como Cítala ou Bastão de Licurgo, e nesse bastão era enrolada uma tira de couro ou papiro, onde era escrita a mensagem. Ao se desenrolar a tira, as letras ficavam desordenadas. Um mensageiro era incumbido de transportar a tira como se fosse um cinto, com as letras voltadas para dentro. Com as letras fora de ordem, mesmo se um inimigo interceptasse a mensagem, esta não poderia ser decifrada. Chegando ao seu destino, o receptor só teria que enrolar a tira num bastão igual ao do emissor e assim conseguiria ler a mensagem facilmente.

Para a época, era uma excelente estratégia de guerra.

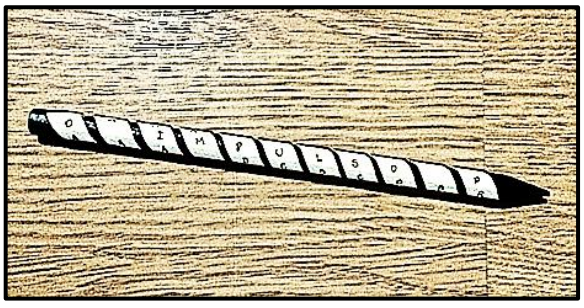
Vejamos na prática como isso funcionava.

Vamos cifrar uma mensagem utilizando uma cítala caseira.

Precisaremos somente de um lápis e uma tira de 1 cm de largura, feita do comprimento de uma folha A4. Enrole a tira no lápis e prenda as pontas com durex.



Eu utilizei um lápis sextavado porque ele tem formato de um prisma regular hexagonal, isso facilita muito na hora de escrever a mensagem.



Exemplo:

Mensagem:

O IMPULSO PARA DESCOBRIR SEGREDOS

ESTÁ NA NATUREZA HUMANA.

O		I	M	P	U	L	S	O		P
A	R	A		D	E	S	C	O	B	R
I	R		S	E	G	R	E	D	O	S
E	S	T	A		N	A		N	A	
T	U	R	E	Z	A		H	U	M	
A	N	A								

Escrevemos a mensagem nas linhas da tabela, dando espaço entre as palavras.

A mensagem cifrada é lida na tira de papel com as letras na ordem que aparecem nas colunas da tabela.

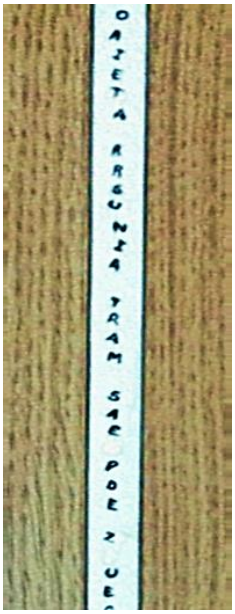
Atenção:

Acentos, cedilha e hífen não são incluídos na cifragem.

Mensagem cifrada por transposição:

OAIETA RRSUNIA TRAM SAE PDE Z UEGNA

LSRA SCE H OODNU BOAM PRS.



Agora observe o título do texto. Ele foi escrito utilizando uma cifra de transposição cuja chave secreta é 312. A chave contem três algarismos, isso significa que as letras foram dispostas em três colunas. Os algarismos simbolizam a numeração das colunas. Para decifrar a mensagem, basta colocar essa numeração em ordem crescente. A quantidade de linhas e colunas da tabela está relacionada à quantidade de letras e espaços entre as palavras da mensagem. O título tem doze letras e uma cifra cuja chave tem três algarismos, logo a tabela utilizada tem três colunas e quatro linhas.

COLUNAS		
3	1	2
A	T	R
P	N	S
I	O	S
O	C	A

⇨

COLUNAS		
1	2	3
T	R	A
N	S	P
O	S	I
C	A	O

Logo, o título decifrado é TRANSPOSIÇÃO.

Esse tipo de criptografia baseia-se no método de cifragem por transposição. Nesse método, as letras da mensagem são permutadas, ou seja, trocadas de lugar. Hoje em dia, não apresenta utilidade criptográfica, pois uma simples análise de frequência torna possível a leitura da mensagem.

Agora é a sua vez!

Usando a tabela abaixo, cifre a mensagem:

NÃO PERMITA QUE O COMPORTAMENTO

DOS OUTROS TIRE SUA PAZ

Chave secreta: 35412

COLUNAS				
1	2	3	4	5

⇨

COLUNAS				
3	5	4	1	2

Mensagem cifrada:

_____

_____

_____

ANEXO C

Texto da Atividade 3

Hikari em:

FULSWRJUDIDQGR

Para criptografar, precisamos usar um sistema criptográfico. A criptografia se utiliza de códigos ou cifras para transformar uma mensagem clara em uma mensagem **ininteligível. Algumas pessoas usam as palavras código e cifra com significados equivalentes, porém são duas coisas diferentes. Um código secreto é um sistema no qual toda palavra ou frase da sua mensagem é substituída por outra palavra, frase ou símbolos, alterando o sentido da mensagem.**

Por exemplo, "A águia está sobrevoando o ninho" pode ser um código para a mensagem "O inimigo está se aproximando".

Uma cifra é um sistema onde cada letra da sua mensagem é trocada por outra letra ou símbolo. A cifra envolve uma chave criptográfica (senha), enquanto o código não. Os códigos podem ser usados em conjunto com as cifras para que as mensagens fiquem ainda mais difíceis de serem decifradas.

As cifras podem ser de chave simétrica ou assimétrica. A cifra de chave simétrica é muito simples. Nesse tipo de criptografia, a chave secreta é única e compartilhada (conhecida) pelo emissor e receptor da mensagem. A chave é usada pelo emissor para cifrar a mensagem antes dela ser enviada e a mesma chave é usada pelo receptor para decifrar a mensagem.

Veja no esquema:

A criptografia de ponta-a-ponta, usada pelo aplicativo Whatsapp, é um exemplo de cifra de chave assimétrica. Nesta, existem duas chaves diferentes: uma pública e a outra privada. A pública é usada pelo emissor para cifrar a mensagem enquanto a chave privada é usada pelo receptor para decifrar a mensagem. A segurança desse tipo de cifra depende do sigilo da chave privada, somente o receptor da mensagem deve conhecê-la.

Uma cifra simétrica que ficou muito famosa na História foi a Cifra de César (50 a.C.). Essa cifra apresentava uma das técnicas mais clássicas de criptografia. César substituía cada letra por outra situada a três posições à frente no alfabeto. Com esse algoritmo, César enganou muitos inimigos do Império Romano.

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

Por exemplo, cifrando a palavra CRIPTOGRAFIA utilizando a Cifra de César teríamos FULSWRJUDILD. Fácil né? Tão fácil que logo foi descoberta pelos inimigos de César e não serviu para mais nada.

Toda cifra simétrica que consiste em substituir uma letra por outra é chamada de cifra de substituição. Quando essa cifra utiliza um único alfabeto cifrante, como é o caso da Cifra de César, ela é classificada como monoalfabética e se usar mais de um alfabeto cifrante é chamada de polialfabética.

Continuando...

A Cifra de César foi descoberta pelos inimigos do Império Romano porque César cometeu um grave erro, utilizou sempre a mesma chave para criptografar suas mensagens, três posições à frente, ou seja, chave 3.

Para não cometermos o mesmo erro, vamos fazer uso de chaves diferentes para cada cifragem!

É muito simples, veja como funciona:

Vamos supor que usemos a chave 10 para criptografar a mensagem SOCORRO.

O primeiro passo é escrever todo o alfabeto, iniciando pelo ***a*** **na posição 10 até o** ***p*** **na** posição 25 e continuando do ***q*** **na posição 0 até o** ***z*** **na posição 9:**

TEXTO CLARO	**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**
CHAVE	**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**
TEXTO CIFRADO	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

Então é só trocar as letras da mensagem pelas letras do alfabeto cifrante. Logo, a mensagem SOCORRO cifrada com a chave 10 é IESEHHE.

Agora é a sua vez, utilize a tabela auxiliar para resolver os exercícios abaixo:

1. Utilizando a chave 22, cifre a mensagem: QUEREMOS PAZ

   _____

2. Utilizando a chave 15, decifre a mensagem: PFEP LXZX FTEZ

   _____

3. Descubra a chave resolvendo o seguinte enigma:

   Sou um múltiplo de 4, antecessor de um número primo e estou entre 14 e 25. Quem sou? _____

   Agora, utilizando a chave encontrada, cifre a mensagem: SALVE O PLANETA.

   _____

4. Agora você será o criptógrafo. Crie uma mensagem curta, escolha uma chave, cifre a mensagem e envie para um colega juntamente com um enigma para que ele possa descobrir a chave e decifrar a sua mensagem.

   Mensagem criada:_____ Chave:_____

   Mensagem cifrada:_____

   Enigma: _____

   Tabela auxiliar:

TEXTO CLARO	**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**
CHAVE	**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**
CIFRA																										

ANEXO D

Texto da Atividade 4

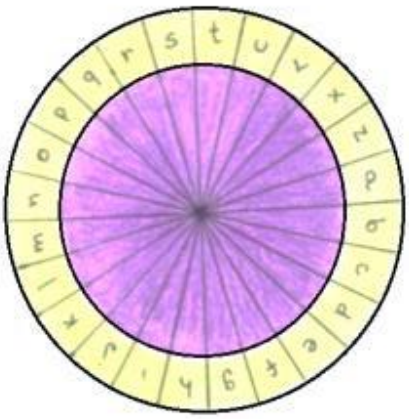
Hikari em:

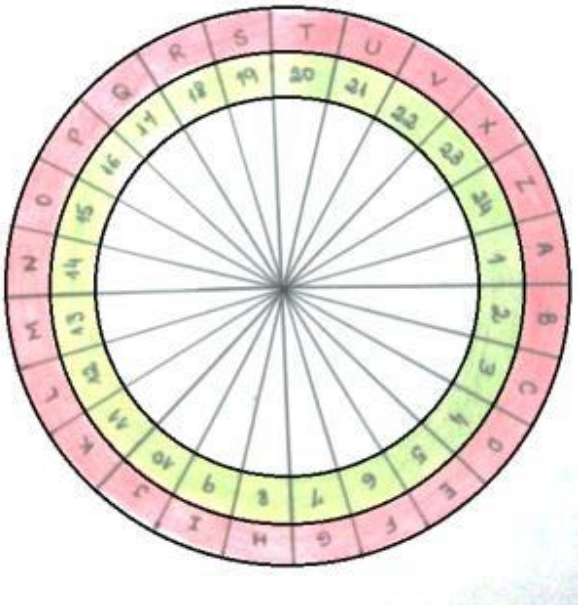
DISCO DE ALBERTI

Leon Battista Alberti, em 1466, foi um dos primeiros a projetar e usar um dispositivo que facilitava o processo criptográfico. Este dispositivo ficou conhecido como Disco de Alberti.

Vamos construir o nosso Disco de Alberti?

O nosso Disco de Alberti é formado por dois círculos como na figura abaixo:





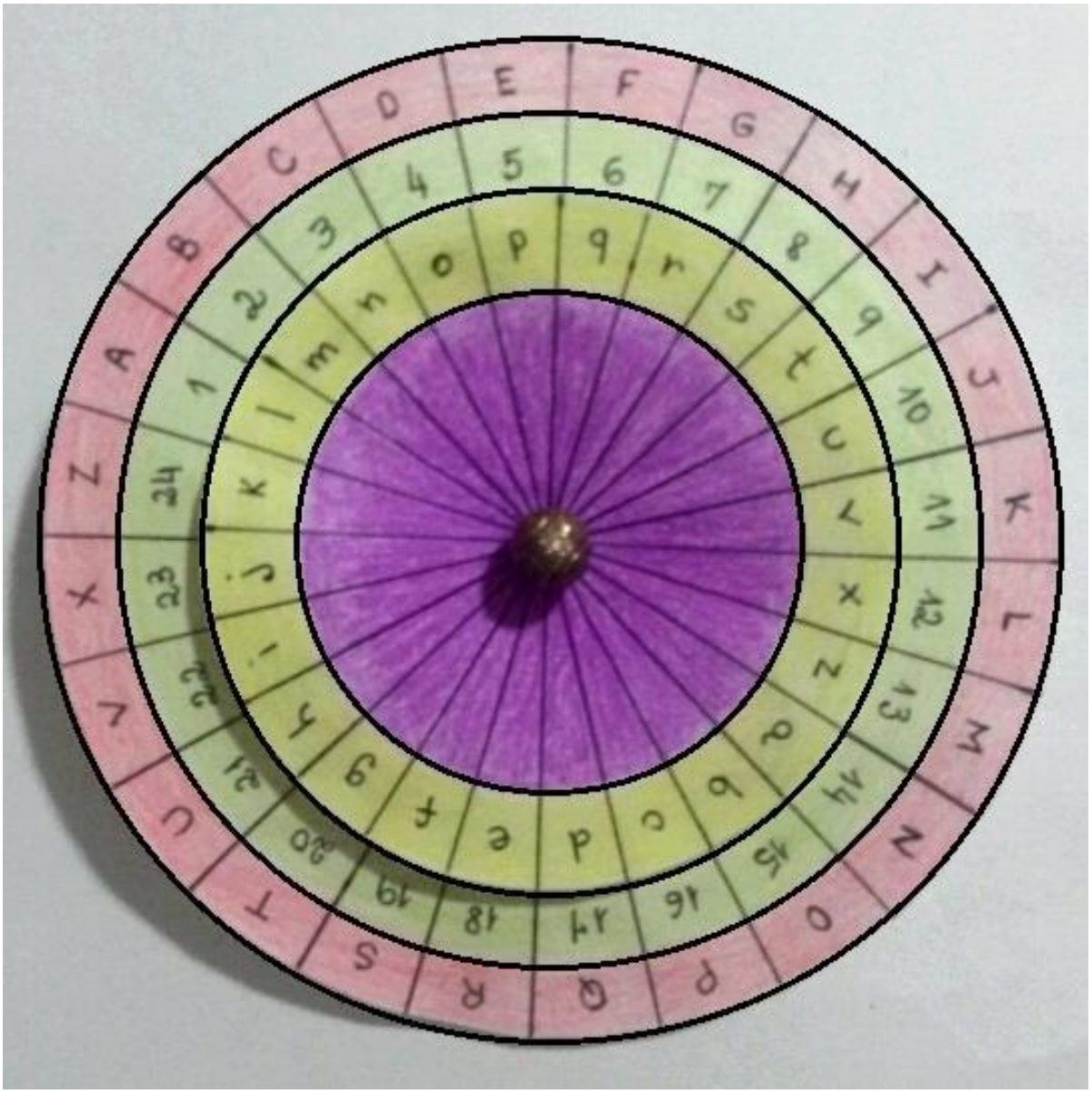
Para construir o primeiro, trace com o compasso três circunferências concêntricas de raios 6 cm, 5 cm e 4 cm. Divida a circunferência externa em 24 partes iguais utilizando um transferidor (360° ÷ 24 = 15°). Trace doze diâmetros. Preencha a primeira coroa circular com as letras do alfabeto, excluindo o W e o Y, pois são as de menor frequência na língua portuguesa. Preencha a segunda coroa circular com os números de 1 até 24. Para o segundo círculo, trace duas circunferências de raios 4 cm e 3 cm. Preencha a coroa circular com as letras do alfabeto, também excluindo o W e o Y.

Se puder colorir, o seu Disco de Alberti ficará lindo!

Depois é só unir os dois círculos com um percevejo ou com um brinco pequeno que tenha em sua casa, use a tarraxa para prender atrás.

Agora nosso Disco de Alberti está pronto!

Vamos fazê-lo funcionar?



Vamos criptografar a palavra: AMOR ETERNO

Escolhe-se uma letra do disco interno. Esta será a letra-chave. Digamos que a letra escolhida seja p. Gira-se o disco interno para alinhar a letra-chave p com uma letra escolhida ao acaso, localizada no disco externo. Para o exemplo, será usada a letra E. Inicia-se o criptograma com a letra E para indicar a posição do disco interno (lembre-se que o p é a chave secreta). As letras da mensagem localizamos no disco externo e, no disco interno, localizamos as letras que devemos substituir. Logo, a letra A será substituída por l, M por z, O por b, R por e, e assim por diante. De acordo com esse processo, teremos a mensagem cifrada: **E lzbe pgpeab.**

Até aqui nenhuma diferença em relação a uma substituição simples. Acontece que Alberti sugere trocar o alfabeto cifrante durante o processo de cifragem, indicando os pontos de troca por letras maiúsculas apontadas pela letra-chave. Assim, se alinharmos a letra p com a letra G, depois de cifrar "AMOR", teremos a mensagem cifrada final: E lzbe G nencxz.

Nesse exemplo, utilizamos dois alfabetos cifrantes, um com a letra-chave na posição E, e o outro na posição G. Por isso que esse tipo de cifra simétrica de substituição recebe a classificação de polialfabética.

Continuando...

Vamos praticar o funcionamento do Disco de Alberti com cifras simétricas de substituição monoalfabéticas e polialfabéticas. A chave numérica deve ser descoberta resolvendo o enigma.

CIFRAS MONOALFABÉTICAS

Exercício 1:

Enigma: Sou um número primo, antecessor de um múltiplo de 5 e compreendido entre 20 e 30.

Chave numérica: _____

Mensagem: WALTER E YAN SÃO IRMÃOS

_____

Exercício 2:

Enigma: Sou o mínimo múltiplo comum entre 12 e 18.

Chave Numérica: _____

Mensagem: O MELHOR ESTÁ POR VIR

_____

Exercício 3:

Enigma: Resolva a expressão $\sqrt{36} + (4^1 \times 3^2)$

Chave Numérica: _____

Mensagem: NUNCA DESISTA

_____

CIFRA POLIALFABÉTICA

Mensagem:

TRANSFORME-SE NA MUDANÇA QUE DESEJA VER

Chave Secreta: d

Enigma 1: Sou o máximo divisor comum entre 9 e 15.

Chave Numérica: _____

Letra da chave numérica: _____

Enigma 2: Resolva a expressão $2^3 + \sqrt{25} \times 20^0$

Chave Numérica: _____

Letra da chave numérica: _____

Enigma 3: Sou um número primo ímpar e sou divisor de todos os números que possuem o algarismo 0 na unidade.

Chave numérica: _____

Letra da chave numérica: _____

Separe a mensagem em três partes, cifre cada parte utilizando a chave secreta alinhada a letra da chave numérica.

1ª parte: TRANSFORME-SE NA

2ª parte: MUDANÇA QUE

3ª parte: DESEJA VER

Mensagem total cifrada:

_____

_____

_____

Molde do Disco de Alberti