UNIVERSIDADE FEDERAL DO OESTE DO PARÁ
INSTITUTO DE CIÊNCIAS DA EDUCAÇÃO
PROGRAMA DE CIÊNCIAS EXATAS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

ELISEU DA ROCHA MARINHO FILHO

CRIPTOGRAFIA: UMA ENGENHARIA DIDÁTICA, COM FUNÇÕES, MATRIZES E CIFRA DE HILL, PARA O ENSINO MÉDIO

SANTARÉM-PA
2016

ELISEU DA ROCHA MARINHO FILHO

CRIPTOGRAFIA: UMA ENGENHARIA DIDÁTICA, COM FUNÇÕES, MATRIZES E CIFRA DE HILL, PARA O ENSINO MÉDIO

Dissertação apresentada ao Programa de Pós-graduação *Matemática em Rede Nacional* – Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade Federal do Oeste do Pará (UFOPA), Instituto de Ciências da Educação, como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Hugo Alex Carneiro Diniz

SANTARÉM-PA
2016

Dados Internacionais de Catalogação-na-Publicação (CIP)
Sistema Integrado de Bibliotecas – SIBI/UFOPA

M337c Marinho Filho, Eliseu da Rocha
Criptografia: uma engenharia didática com funções matrizes e cifra de Hill, para o ensino médio. / Eliseu da Rocha Marinho Filho. – Santarém, 2015.
128 fls.: il.
Inclui bibliografias.
Orientador Hugo Alex Carneiro Diniz
Dissertação (Mestrado) – Universidade Federal do Oeste do Pará, Instituto de Ciências da Educação, Programa de Ciências Exatas, Mestrado Profissional em Matemática em Rede Nacional.

1. Criptografia. 2. Engenharia didática. 3. Funções. 4. Matrizes. 5. Cifras de Hill. I. Diniz, Hugo Alex Carneiro, orient. II. Título.

CDD: 23 ed. 005.82

Bibliotecário - Documentalista: Eliete Sousa – CRB/2 1101

ELISEU DA ROCHA MARINHO FILHO

CRIPTOGRAFIA: UMA ENGENHARIA DIDÁTICA, COM FUNÇÕES, MATRIZES E CIFRA DE HILL, PARA O ENSINO MÉDIO

Dissertação apresentada ao Programa de Pós-graduação *Matemática em Rede Nacional* – Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade Federal do Oeste do Pará (UFOPA), Instituto de Ciências da Educação, como requisito parcial para a obtenção do título de Mestre em Matemática.

Parecer da Banca:_____ em, ___ de _____ de 2016

Banca Examinadora:

_____

Prof. Dr. Hugo Alex Carneiro Diniz
Orientador – UFOPA

_____

Prof. Dr. João Cláudio Brandemberg Quaresma
Examinador – UFPA

_____

Prof. Msc. Aroldo Eduardo Athias Rodrigues
Examinador – UFOPA

SANTARÉM-PA
2016

DEDICATÓRIA

À Clara Marinho, porto seguro em tempos de tempestade, por todo apoio e compreensão.

AGRADECIMENTOS

Agradeço a Deus ...

Ao meu orientador ...

Aos meus familiares ...

Aos professores da UFOPA...

Aos funcionários da Escola Belo de Carvalho...

Aos meus amigos...

Aos alunos que participaram do experimento...

A todos que de forma direta ou indireta participaram desta conquista.

“O insucesso é apenas uma oportunidade para recomeçar de novo com mais inteligência.”

Henry Ford.

RESUMO

O presente trabalho apresenta a aplicação de uma sequência didática com o tema Criptografia envolvendo os conteúdos de Funções e Matrizes do Ensino Médio e, introduzindo conteúdos novos, como cálculo de inversa de Funções Quadráticas e tópicos de Aritmética Modular, bem como incentivando a utilização da calculadora científica como instrumento facilitador para cálculos longos. Criptografia é o estudo dos princípios e técnicas pelas quais uma informação pode ser transformada (codificada) da sua forma original para outra ilegível. As transações comerciais modernas e a comunicação entre pessoas necessitam de sigilo, em virtude disto, faz-se necessário um estudo das várias formas de se criptografar uma mensagem ou uma informação que se deseja enviar, a fim de que esta não seja lida pela "pessoa errada". As hipóteses foram: existe uma relação entre o tema Criptografia e a Matemática do Ensino Médio; a abordagem de conteúdos matemáticos do Ensino Médio associados à Criptografia pode trazer uma maior assimilação desses conteúdos. A problemática pesquisada foi como desenvolver uma sequência didática que apresentasse a Matemática como uma ferramenta que pudesse ser amplamente aplicada à codificação das transações e comunicações humanas, ou seja, à Criptografia. O objetivo geral desta pesquisa foi a implementação de uma Engenharia Didática, para o tratamento do tema Criptografia, associado aos conteúdos de Matemática trabalhados no Ensino Médio. Os objetivos específicos, para atingir o objetivo geral, foram: revisão teórica sobre a história da Criptografia; mostrar como a Criptografia se relaciona com o nosso cotidiano; estabelecer as principais formas de se criptografar uma mensagem, dando enfoque às que usam conteúdos do Ensino Médio; Criar uma sequência didática que pudesse ser aplicada ao 2º ano do Ensino Médio, usando Funções, Matrizes e Aritmética Modular. A utilização da Engenharia Didática, como metodologia da pesquisa, possibilitou que a análise dos dados fosse feita internamente, validando as atividades desenvolvidas. A Engenharia Didática, vista como metodologia de pesquisa, é um esquema experimental baseado em "realizações didáticas" em sala de aula, ou seja, na concepção, realização, observação e análise de uma sequência de ensino. Desenvolveu-se as quatro fases da Engenharia Didática, quais sejam: análises preliminares; concepção e análise a priori; experimentação; análise a posteriori e validação. A fase de experimentação foi desenvolvida na Escola Estadual Belo de Carvalho, do município de Santarém-Pa. Os resultados indicam que a sequência didática com o tema Criptografia possibilitou aos alunos associar os conteúdos matemáticos trabalhados, no ensino médio, a um tema atual e de relevância para o cotidiano deles. Possibilitou ainda, revisar conteúdos que já haviam sido esquecidos, além de obter o conhecimento de conteúdos novos. Permitiu uma maior interação entre os alunos, além de promover o trabalho em grupo e a divisão de tarefas para a realização de um objetivo. Também possibilitou desenvolver as capacidades de concentração nas atividades e de criação de estratégias de resolução de problemas.

Palavras-chave: Criptografia. Engenharia Didática. Funções. Matrizes. Cifras de Hill.

ABSTRACT

This paper presents the application of a didactic sequence with the theme Cryptography involving High School Functions and Matrices of content and by introducing new content, such as inverse calculation Quadratic Functions and topics Modular Arithmetic, as well as encouraging the use of the calculator scientific as facilitator for long calculations. Cryptography is the study of the principles and techniques by which the information may be transformed (encoded) from its original form to another unreadable. Modern business transactions and communication between people require secrecy, because of this, it is necessary a study of the various ways to encrypt a message or information you want to send, so that this is not read by the "wrong person". The hypotheses were: there is a relationship between the theme Cryptography and Mathematics high school; the approach of mathematical content of high school associated with encryption can bring greater assimilation of such content. The researched problem was how to develop a didactic sequence to present mathematics as a tool that could be widely applied to the coding of transactions and human communications, ie the encryption. The objective of this research was the implementation of a Didactic engineering, addressing the topic Encryption, combined with mathematics content worked in high school. The specific objectives to achieve the overall goal, were: theoretical review of the history of cryptography; show how the encryption is related to our daily life; establish the main ways to encrypt a message, by focusing on using high school content; Create a teaching sequence that could be applied to the 2nd year of high school, using Functions, Arrays and Modular Arithmetic. The use of the Didactic Engineering as research methodology, enabled the analysis of the data was done internally validating the activities. The Didactic Engineering, seen as research methodology is an experimental scheme based on "educational achievements" in the classroom, or in the design, implementation, observation and analysis of a teaching sequence. Developed the four stages of Didactic Engineering, namely: preliminary analysis; design and analysis a priori; experimentation; posteriori analysis and validation. The trial phase was developed in the State School Belo de Carvalho, the municipality of Santarém-Pa. The results indicate that the teaching sequence with the topic Encryption enabled students associate the mathematical contents worked in high school, a current theme and relevance to their daily lives. Possible further review content that had been forgotten, and gain knowledge of new content. Allowed greater interaction among students and promote group work and the division of tasks for the achievement of a goal. Also possible to develop the capacities of concentration in the activities and the creation of problem-solving strategies.

Key-words: Encryption. Didactic Engineering. Functions. Matrices. Ciphers Hill.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

Segundo os Parâmetros Currículares Nacionais (PCN's) Brasil (2000) e a Lei de Diretrizes e Base da Educação Nacional (LDB) Brasil (2015), o ensino/aprendizado de Matemática deve ter como principal objetivo a formação social do aluno. Esta formação está associada a inserção deste no mercado de trabalho, na cultura e nas interações sociais. O mercado de trabalho de hoje exige cada vez mais profissionais que saibam exercer papéis de liderança, de trabalho em grupo, de criatividade, para resolver os mais diferentes problemas. Nesse contexto, a Matemática tem importante papel ao promover uma educação que proporcione ao aluno o contato com desafios que possam desenvolver essas qualidades.

A palavra *Criptografia*, em sua etimologia, é a junção de duas palavras gregas, *kryptós* que significa oculto, secreto, escondido e *gráphein* que significa escrita. De acordo com Olgin, Groenwald e Franke (2011), Criptografia é o estudo dos princípios e técnicas pelas quais uma informação pode ser transformada (codificada) da sua forma original (plaintext) ou texto claro (cleartext) para outra ilegível, chamada texto cifrado (ciphertext), texto código (codetext) ou simplesmente cifra (cipher), que usualmente tem a aparência de um texto randômico (aleatório) ilegível, de forma que possa ser conhecida apenas por seu destinatário, que é o detentor de uma "chave" capaz de decodificar a informação, possibilitando a sua leitura. Segundo Coutinho (2009), embora algumas pessoas ainda associem mensagens codificadas à agentes secretos, há mais de uma década que esta não é a aplicação mais importante da Criptografia. Hoje em dia, operações de serviços disponíveis na internet, movimentações bancárias, transações em terminais eletrônicos, ou seja, todas as transações que envolvem dinheiro e que são feitas por meios eletrônicos, necessitam da criptografia para uma comunicação de forma confidencial. Ainda segundo Coutinho (2009), os processos pelos quais informações são codificadas dependem, de maneira geral, do uso da Matemática. Sobre o crescimento da Criptografia, Zatti e Beltrame (2006) dizem que, atualmente, a Criptografia, dado o grau de sofisticação e embasamento teórico que envolve o seu estudo, é considerada uma ciência, no campo das Ciências Exatas.

Além da Criptografia, segundo Olgin, Groenwald e Franke (2011), temos a *Criptoanálise* (kriptós = escondido, oculto; análysis = decomposição) que é a arte ou ciência de determinar a chave cifradora ou decifrar mensagens sem conhecer a chave, uma tentativa de Criptoanálise é chamada ataque. *Criptologia* (kriptós = escondido, oculto; logo = estudo, ciência) é a ciência que reúne a Criptografia e a Criptoanálise. Ainda para Olgin, Groenwald e Franke (2011), *cifrar* é o ato de transformar dados em alguma forma ilegível. Seu propósito é

o de garantir a privacidade, mantendo a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados. *Decifrar* é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível. De acordo com Stein (2011, apud RIBEIRO, LOURENÇANO e COSTA, 2013) de maneira geral, há um emissor que tenta enviar uma mensagem para um receptor, existe também um adversário que deseja interceptar essa mensagem. Além disso, para Olgin, Groenwald e Franke (2011), para cifrarmos ou decifrarmos uma mensagem, necessitamos de informações confidenciais geralmente denominadas chaves ou senhas. Dependendo do método de criptografia empregado, a mesma chave pode ser utilizada tanto para criptografar como para decriptografar (decodificar, desincriptar, ler) mensagens, enquanto outros mecanismos utilizam senhas diferentes.

As transações comerciais modernas e a comunicação entre pessoas necessitam de sigilo, em virtude disto, faz-se necessário um estudo das várias formas de se criptografar uma mensagem ou uma informação que se deseja enviar, afim de que esta não seja lida pela "pessoa errada". Durante o Ensino Médio não são abordados, de forma eficiente, temas que têm grande relevância para o cotidiano dos alunos, levando estes a concluir que a matemática é desconexa de sua vida, algo enfadonho que só é estudado por obrigação.

O estudo da Criptografia é importante em várias formas de transações e comunicações entre pessoas, mesmo assim não é trabalhado com alunos do Ensino Médio.

As principais hipóteses levantadas neste trabalho foram as seguintes: existe uma relação entre o tema Criptografia e a Matemática do Ensino Médio; a abordagem de conteúdos matemáticos do Ensino Médio, especialmente Funções e Matrizes, associados à Criptografia e sua história pode trazer uma maior assimilação desses conteúdos.

A principal problemática pesquisada foi como desenvolver uma sequência didática, para ser aplicada no segundo ano do Ensino Médio, que apresentasse a Matemática como uma ferramenta que pudesse ser amplamente aplicada à codificação das transações e comunicações humanas, ou seja, à Criptografia.

Segundo Tamarozzi (2001, apud GROENWALD e FRANKE, 2008) o tema Criptografia possibilita o desenvolvimento de atividades didáticas envolvendo o conteúdo de funções e matrizes que se constituem em material útil para exercícios, atividades e jogos de codificação, podendo o professor utilizá-los para fixação de conteúdos. Aliado a isso, de acordo com Groenwald e Olgin (2010) trabalhar com atividades metodológicas utilizando códigos e senhas oportuniza aos alunos reforçar os conteúdos matemáticos já estudados,

utilizar a calculadora como um recurso facilitador para cálculos longos, e ainda favorece o trabalho em grupo.

O objetivo geral desta pesquisa foi a implementação de uma Engenharia Didática, para o tratamento do tema Criptografia, associado aos conteúdos de Matemática trabalhados no Ensino Médio. A Engenharia Didática (como veremos melhor no capítulo 4), vista como metodologia de pesquisa, é um esquema experimental baseado em "realizações didáticas" em sala de aula, ou seja, na concepção, realização, observação e análise de uma sequência de ensino.

Os objetivos específicos, para atingir o objetivo geral, foram: revisão teórica sobre a história da Criptografia; mostrar como a Criptografia se relaciona com o nosso cotidiano; estabelecer as principais formas de se criptografar uma mensagem, dando enfoque às que usam conteúdos do Ensino Médio; criar uma sequência didática que pudesse ser aplicada ao 2º ano do Ensino Médio, usando Funções, Matrizes e Aritmética Modular; fazer com que a Criptografia seja conhecida por professores e alunos do Ensino Médio e, que os professores possam trabalhar, posteriormente, esse tema com seus alunos, de forma motivadora com exemplos do dia a dia das transações e comunicações entre pessoas, de tal maneira que se possa instigar o aluno a pesquisar mais sobre o assunto e conteúdos matemáticos associados; estimular o uso da calculadora como instrumento facilitador para cálculos longos; melhorar a absorção dos conteúdos Funções e Matrizes com a utilização do tema Criptografia.

Apresenta-se neste trabalho a Criptografia como um instrumento facilitador da construção de conceitos matemáticos e como um catalisador do interesse do estudante acerca de conteúdos de Matemática Básica trabalhados no Ensino Médio. Entretanto, o tópico Criptografia é muito vasto e, consequentemente, correr-se-ia o risco de se tornar superficial demais ao tentar abordar o conteúdo todo. Para especificar um pouco mais o campo de estudo, encontra-se neste trabalho, um tratamento das formas mais importantes de se criptografar uma mensagem, enfocando as formas mais básicas que usam ferramentas matemáticas elementares, que podem ser trabalhadas em sala de aula com alunos do segundo ano do Ensino Médio, como Divisões Euclidianas, Potências, Funções Afins, Funções Quadráticas, Funções Exponenciais, Funções Logarítmicas e Matrizes.

Para um entendimento maior dos conteúdos matemáticos associados aos tópicos de Criptografia abordados neste trabalho recomendamos a seguir algumas leituras. Para uma compreensão maior de Funções, Função Afim, Função Quadrática, Função Exponencial e Função Logarítmica recomendamos a leitura de (LIMA, CARVALHO, *et al.*, 2006), (IEZZI e MURAKAMI, 2013) e (DOLCE, IEZZI e MURAKAMI, 2013). Para um maior entendimento

sobre Matrizes recomendamos a leitura de (LIMA, CARVALHO, *et al.*, 2006) e (HAZZAN e IEZZI, 2012). Por fim, para um maior aprendizado sobre tópicos de Aritmética recomendamos a leitura de (HEFEZ, 2011), (SANTOS, 2014), (HEFEZ, 2009), (SIDKI, 2009), (ALENCAR, 2013) e (COUTINHO, 2009).

No segundo capítulo deste trabalho você encontrará um histórico da Criptografia. No terceiro temos uma evolução da criptografia na "era dos computadores", de que forma a criptografia evolui junto aos computadores, desde o surgimento destes. O quarto capítulo apresenta as metodologias utilizadas na elaboração deste trabalho. No quinto capítulo apresentamos as atividades propostas para serem aplicadas em sala de aula. O sexto e último capítulo é onde apresentamos a nossa experiência com a aplicação das atividades com os alunos do 2º ano do ensino médio da Escola Estadual de Ensino Fundamental e Médio Antônio Batista Belo de Carvalho da cidade de Santarém-Pa.

Ao longo deste trabalho buscamos sempre trazer a Criptografia e a Matemática para a vida dos alunos e professores de forma clara e objetiva, para que possa se tornar de fácil compreensão, objetivando transformar este trabalho em mais um instrumento que possa ser utilizado por professores e alunos no processo de ensino/aprendizagem.

2 HISTÓRICO DA CRIPTOGRAFIA

Desde os tempos antigos o ser humano já sentia necessidade de enviar mensagens secretas que só pudessem ser lidas pelas “pessoas certas”, sem que a mensagem caísse em “mãos erradas”. Essa ideia de enviar mensagens “ocultas” surgiu principalmente da necessidade do homem de se comunicar durante uma guerra, para que pudesse transmitir mensagens fundamentais para a vitória no campo de batalha, como a posição do inimigo, mantimentos, munições e etc. A respeito disso Quaresma (2008) e Shokranian (2005, apud GROENWALD e OLGIN, 2010) dizem que a necessidade de proteger os canais de comunicação entre pessoas de uma mesma comunidade vem desde os primórdios da civilização, a ideia de não só proteger os meios de comunicação, mas também de proteger o próprio conteúdo da mensagem, através da cifração, é também muito antiga. Ainda sobre o assunto Tamarozzi (2001, apud OLGIN, 2011) afirma que a Criptografia é bastante antiga, pois já havia indícios, no sistema de escrita hieroglífica dos egípcios e dos romanos, da utilização de códigos secretos para transmitir seus planos de batalha. Para Santos (2013) a escrita hieroglífica (Figura 1: Escrita Hieroglífica), compreensível apenas aos sacerdotes egípcios, que data de 2000 a. C., é o primero indício histórico da preocupação do homem em tornar textos ininteligíveis. Ainda segundo o autor, a escrita cuneiforme (Figura 2: Escrita Cuneiforme), dos babilônios, ratifica essa tese.

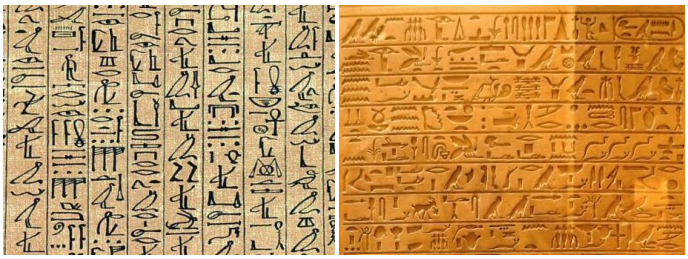


Figura 1: Escrita Hieroglífica
Fonte: http://sul.colmaster.com.br/projetohumanas/wp-content/uploads/2015/03/escrita-hieroglifica.jpg

Figura 2: Escrita Cuneiforme
Fonte: http://www.portalsaofrancisco.com.br/alfa/civilizacao-sumeria/imagens/Escrit32.jpg

2.1 Heródoto e a Esteganografia

Segundo Marques (2013) um dos primeiros textos sobre códigos secretos foi escrito pelo geógrafo e historiador grego Heródoto (485 a.C. – 420 a.C.), "o pai da história", (Figura 3: Heródoto,"O Pai da História"). Ele foi o primeiro não só a escrever sobre o passado, mas também a considerar o passado como um problema filosófico ou um projeto de pesquisa que podia revelar conhecimento do comportamento humano. Ainda segundo o autor, na sua obra principal ("As Histórias", de Heródoto), são retratados os conflitos entre a Pérsia e a Grécia, no século V a.C., nela, Heródoto, atribui à escrita secreta a causa de a Grécia não ter sido conquistada por Xerxes. Para Freire e Castilho (2007) a estratégia utilizada pelos persas era de se organizarem secretamente para combater os gregos, seu plano era o ataque surpresa, no entanto, não contavam que a Grécia usasse uma arma mais forte que era a arte da escrita secreta. De acordo com Marques (2013), Demarato, um grego que vivia exilado na Pérsia, teve acesso aos planos de Xerxes (rei dos Persas) e resolveu avisar aos espartanos. Vejamos um trecho da história narrada pelo próprio Heródoto:

> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareciam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os gregos (SINGH, 2007, apud MARQUES, 2013, p. 2).

Segundo Santos (2013) a mensagem chegou ao seu destino e cumpriu o seu objetivo, pois os gregos, até então indefesos, se armaram e humilharam a esquadra persa em um contra-ataque surpresa.

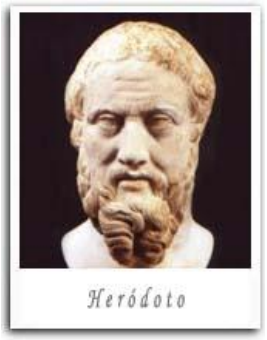


Figura 3: Heródoto,"O Pai da História"
Fonte: http://www.portaltattoo.com/conteudo/tatuagem/herodoto.jpg

Outro acontecimento importante na área da *Esteganografia* é também narrado no livro "As Histórias" de Heródoto. Segundo Marques (2013), é a história de Histaeu, que queria encorajar Aristágora de Mileto a se revoltar contra o rei Persa. De acordo com Santos (2013), Histaeu raspou a cabeça de um de seus escravos, escreveu a mensagem em seu couro cabeludo e esperou o cabelo crescer novamente. O mensageiro, quando chegou ao seu destino, raspou a cabeça novamente, revelando a mensagem escondida.

As duas histórias exibidas acima, narradas por Heródoto, são exemplos de uma técnica de ocultação de mensagem chamada *Esteganografia*. De acordo com Loureiro (2014) uma das primeiras técnicas para trazer privacidade a uma troca de informações foi a Esteganografia. Segundo Santos (2013), Esteganografia é a arte de esconder uma mensagem, sem nenhum tratamento para modificá-la, que deriva do grego *steganos*, escondido, coberto, e *graphia*, escrita. Ainda segundo Loureiro (2014), a Esteganografia é uma ciência irmã da Criptografia.

Diversas técnicas esteganográficas surgiram ao longo dos anos. Segundo Marques (2013) entre alguns exemplos estão a escrita de uma mensagem secreta em uma tira de seda fina, que era amassada formando uma pequena bola, coberta com cera e engolida por um mensageiro. Ainda segundo o autor, outra forma seria a tinta invisível usada na escrita que, após um suave aquecimento, adere a cor marrom. E, por fim, o autor cita a mensagem no ovo cozido que, baseava-se em escrever uma mensagem sobre a casca de um ovo com uma tinta especial que penetrava em sua casca e estampava o ovo. Por outro lado, Loureiro (2014) e Santos (2013) afirmam que um exemplo é o *microponto*, que consiste em reduzir uma foto de um texto até transformá-la em um ponto. O microponto era então oculto sobre o ponto final de uma carta aparentemente inofensiva. O receptor, ao receber a mensagem, procurava pelo ponto e ampliava-o para ter acesso a informação. Sobre o assunto Singh (2011, apud LOUREIRO, 2014) nos conta que esta técnica foi praticada pelos alemães durante a segunda guerra mundial. Segundo Santos (2013) os aliados descobriram a técnica em 1941 e passaram

a interceptar a comunicação, isso forçou os alemães a desenvolverem outras técnicas para esconder suas mensagens.

Para Loureiro (2014) a diferença entre esteganografia e a criptografia é que, o objetivo da primeira é de esconder a mensagem, enquanto o da segunda é de ocultar o significado da mensagem. Segundo Stallings (2004, apud LOUREIRO, 2014) a vantagem da criptografia sobre a esteganografia é que, se o inimigo interceptar a mensagem ela estará codificada, logo será ininteligível e o seu conteúdo não será revelado. Ainda para o mesmo autor, atualmente, em alguns casos, se usa uma combinação das duas técnicas a fim de oferecer mais segurança. Sobre o assunto Santos (2013) nos conta, ao se referir ao episódio do microponto dos alemães, que após a descoberta dos aliados, os alemães passaram a tomar a precaução extra de codificar a mensagem antes de microfilmá-la.

2.2 O Citale Espartano, a Tabela Espartana, a Cifra de Políbio e as Cifras Monoalfabéticas

De acordo com Singh (2003, apud GROENWALD e OLGIN, 2010), ao longo da história, foram utilizados diversos mecanismos de codificação e decodificação, denominados códigos, cifras e senhas, um exemplo é o *Citale Espartano* ou *Bastão de Licurgo*, que foi um aparelho criptográfico militar, que consistia em um bastão de madeira, onde se enrolava uma tira de couro e se escrevia a mensagem em todo o comprimento desse bastão. Segundo o autor, para enviar a mensagem, de forma despercebida, a tira de couro era desenrolada do citale e utilizada como cinto, com a mensagem voltada para dentro. Como na tira de couro a mensagem ficava sem sentido, para decifrá-la era necessário que o receptor tivesse um citale de mesmo diametro para enrolar a tira de couro e ler a mensagem, conforme Figura 4: Citale Espartano.

Figura 4: Citale Espartano
Fonte: https://upload.wikimedia.org/wikipedia/commons/thumb/5/51/Skytale.png/199px-Skytale.png

Um método utilizado na Grécia antiga, conforme descrito por Plutarco, em 90 d. C., no livro *"Vida de Homens Ilustres"*, era a *Tabela Espartana*, que consiste de uma tabela

comum, onde a chave do código era o número de colunas da tabela, já que o número de linhas dependeria do tamanho da mensagem (SANTOS, 2013, p. 17). Ainda segundo o autor a mensagem era escrita nas células da tabela, da esquerda para a direita e de cima para baixo (ou de outra forma previamente combinada) e o texto cifrado era obtido tomando-se as letras em outro sentido e direção. Para entendermos um pouco melhor, tomemos a mensagem "A MATEMÁTICA MUDOU MINHA VIDA" e vamos distribuí-la em uma tabela de 5 colunas, utilizando a letra H no lugar dos espaços, ficamos com a seguinte tabela (Tabela 1: Exemplo de Tabela Espartana).

A	H	M	A	T
E	M	A	T	I
C	A	H	M	U
D	O	U	H	M
I	N	H	A	H
V	I	D	A	H

Tabela 1: Exemplo de Tabela Espartana
Fonte: Do Autor

Agora, tomando o texto de cima para baixo nas colunas, e agrupando em blocos de 5 letras (de acordo com o número de colunas), obtemos o seguinte texto ininteligível:

AECDI VHMAO NIMAH UHDAT MHAAT IUMHH

Quando a quantidade de letras do texto não for múltipla de 5, completa-se o último bloco do texto ininteligível com letras aleatórias (SANTOS, 2013, p. 18).

A *Cifra de Políbio* data de 200 a. C., seu funcionamento se baseia no uso da tabela abaixo (veja Tabela 2: Cifra de Políbio) em que cada letra passa a ter como representação duas outras, duplicando a extensão da mensagem original (DAINEZE, 2013, p. 26).

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

Tabela 2: Cifra de Políbio
Fonte: (DAINEZE, 2013)

Utilizando esta tabela, substituímos o "A" por "AA" o "B" por "AB" e assim sucessivamente. As letras "I" e "J" têm a mesma cifração, assim, quando se proceder a decifração da mensagem codificada, escolhe-se aquela que dá significado ao texto (FIARRESGA, 2010, p. 25).

Segundo Fiarresga (2010) há ainda outra versão desta mesma cifra em que as letras A, B, C, D e E, utilizadas para codificar as mensagens, são trocadas pelos números 0, 1, 2, 3 e 4, formando a seguinte tabela (veja Tabela 3: Cifra de Políbio (Variação)).

	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I/J	K
2	L	M	N	O	P
3	Q	R	S	T	U
4	V	W	X	Y	Z

Tabela 3: Cifra de Políbio (Variação)
Fonte: (FIARRESGA, 2010)

Ainda segundo Fiarresga (2010), Políbio sugeriu que se aproveitasse esta tabela para transmitir mensagens utilizando tochas. A mensagem era transmitida letra por letra. Por exemplo, para transmitir a letra "H" (que corresponde ao número 12), o mensageiro segurava na mão direita uma tocha e, na esquerda, duas.

Já para Costa (2014), as letras A, B, C, D e E deveriam ser substituídas pelos números 1, 2, 3, 4 e 5. Para criptografar por esse método, bastaria associar a cada letra um

número de dois dígitos formado pela linha e pela coluna, nessa ordem, onde estava a letra (como uma matriz 5x5). Por exemplo, a letra “L” está representada pelo número 31.

Ainda segundo o autor, o quadro de Políbio apresentava uma maneira de associar letras a números, mas não era fixo, senão não teria utilidade, visto que todos que o usassem uma vez sempre saberiam como decifrar as mensagens. As letras poderiam ser colocadas no interior do quadro, de maneira aleatória, o que daria inúmeras possibilidades de variação da cifra.

O primeiro relato sobre uma cifra de substituição, onde as letras do texto claro são substituídas por outras, aparece no *Kama-sutra* (LOUREIRO, 2014, p.4). Segundo Olgin, Groenwald e Franke (2011) no *Kama-sutra*, texto escrito no século IV pelo estudioso brâmane Vatsyayana, baseado em manuscritos que datam do século IV a. C, recomenda-se que as mulheres devem estudar 64 artes, entre elas, culinária, vestuário e etc. O número 45 dessa lista é a *mlecchita-vikalpa*, a arte da escrita secreta, para que fosse possível, para a mulher, esconder detalhes de seus relacionamentos amorosos (SINGH, 2011, apud LOUREIRO, 2014, p. 4). A técnica consistia em um aparelhamento ao acaso das letras do alfabeto, substituindo-se cada letra da mensagem original por seu par (LOUREIRO, 2014, p. 4).

Qualquer forma de criptografar, utilizando a substituição de uma letra por outra ou por um símbolo é denominada de *cifra* (OLGIN, GROENWALD e FRANKE, 2011). Para Singh (2003, apud OLGIN, GROENWALD e FRANKE, 2011), Júlio César utilizava-se da cifra para fins militares, existem registros em que César descreve como enviou uma mensagem para Cícero, que estava cercado pelos inimigos e prestes a se render. Nesta mensagem Júlio César substituiu as letras do alfabeto romano por letras gregas. Assim, o primeiro documento que usou uma cifra de substituição para propósito militar foi feito pelo imperador romano Júlio César (LOUREIRO, 2014, p. 4).

De acordo com Olgin, Groenwald e Franke (2011), outro tipo de cifra utilizada por Júlio César consistia em substituir cada letra da mensagem original por outra que estivesse três casas à frente no mesmo alfabeto. César utilizava o alfabeto normal para escrever a mensagem e o alfabeto cifrado era utilizado para codificar a mensagem que mais tarde seria enviada (veja Tabela 4: Cifra de César).

Texto simples	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifra	D	E	F	G	H	I	J	K	L	M	N	O	P
Texto simples	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifra	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabela 4: Cifra de César
Fonte: http://www.recantododragao.com.br/wp-content/uploads/2013/04/Sem-t%C3%ADtuloee1.png

Após um tempo, a denominação de *Código de César* ou *Cifra de César* passou a designar qualquer cifra na qual cada letra da mensagem seja substituída por outra deslocada um número fixo de posições (DAINEZE, 2013, p. 27). Singh (2002, apud FREIRE e CASTILHO, 2007) afirma que este método é considerado um dos mais simples e se deve à necessidade que o imperador tinha de se comunicar com suas legiões que se encontravam espalhadas pela Europa, Ásia e África. Esses tipos de Criptografias por substituição, que empregam somente um alfabeto, são chamadas de *Cifras Monoalfabéticas*. Na cifra de César, para dificultar a decodificação, removem-se os espaços entre as palavras no texto cifrado. Singh (2003, apud OLGIN, 2011) relata que essa não é uma cifra segura, pois possui 25 chaves em potencial. Logo, ao ser interceptada a mensagem, sabendo-se que se trata de uma Cifra de César, será necessário verificar apenas 25 chaves para decodificá-la.

Códigos como os de César padecem de um grande problema: são muito fáceis de "quebrar". Quebrar um código significa ser capaz de ler a mensagem, mesmo não sendo seu destinatário legítimo (COUTINHO, 2009, p. 10). Na verdade qualquer código que envolva substituir cada letra sistematicamente por outro símbolo sofre do mesmo problema (COUTINHO, 2009, p. 10).

2.3 A Criptoanálise e as Cifras Polialfabéticas

Segundo Loureiro (2014), paralelamente ao desenvolvimento da criptografia, ocorre o desenvolvimento da *Criptoanálise* que é a ciência que estuda as técnicas para obtenção da informação sobre a mensagem original, a partir do texto cifrado. São as técnicas usadas para se "quebrar" a mensagem cifrada.

De acordo com Marques (2013), no século IX, um matemático árabe, que trabalhava na "Casa da Sabedoria de Bagdad", escreveu um livro manuscrito sobre o deciframento de mensagens criptográficas. O nome desse árabe era *Al-Kindi* (veja Figura 5: Imagem de Al-

Kindi), conhecido como o “filósofo dos árabes”. Seu maior tratado só foi descoberto em 1987, no Arquivo Otomano Sulaimaniyyah em Istambul, e se intitula: *“Um Manuscrito Sobre a Decifração de Mensagens Criptográficas”*.

Figura 5: Imagem de Al-Kindi
Fonte: https://40.media.tumblr.com/dea60ef5708619f7c5afc71ed3ab870e/tumblr_mux0rddiKw1sqh30oo1_400.jpg

Nesse livro é descrito um método para decifrar mensagens, utilizando a *Análise de Frequências*. Quando contamos a frequência com que as letras aparecem em um texto longo, em qualquer idioma, descobrimos uma frequência relativa (DAINEZE, 2013, p. 27). Assim, contando-se os símbolos na mensagem cifrada e, sabendo-se o idioma do texto original, basta comparar a frequência dos símbolos com uma tabela de frequência previamente elaborada (ALENCAR, 2013, p. 35). Obviamente que algumas suposições e avaliações sobre o texto cifrado ainda terão que ser feitas, mas a quantidade de tentativas diminui consideravelmente (SANTOS, 2013, p. 19). Por exemplo, a frequência média de cada letra, na língua portuguesa, é apresentada na tabela abaixo (Figura 6: Frequência Relativa das Letras na Língua Portuguesa).

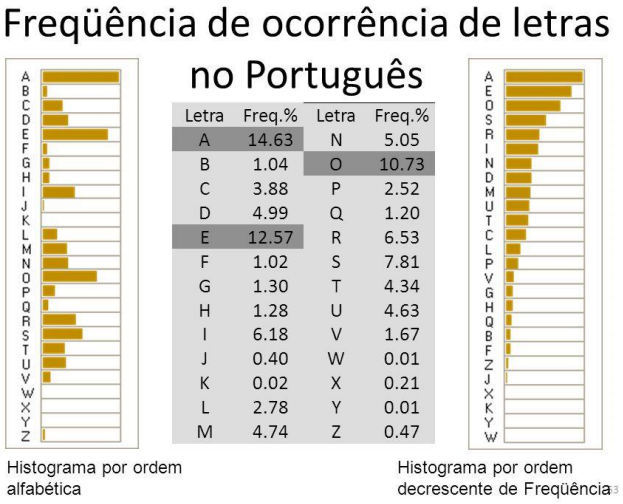


Figura 6: Frequência Relativa das Letras na Língua Portuguesa
Fonte: http://images.slideplayer.com.br/3/383339/slides/slide_53.jpg

Para decodificar o texto cifrado, basta contar a frequência de cada símbolo no texto para descobrir a quais letras correspondem os símbolos mais frequentes. Isto geralmente é suficiente para quebrar o código e ler toda a mensagem (MARQUES, 2013, p. 7). Por exemplo, se em um texto cifrado identificarmos que as maiores frequências são das letras W, M e P, então as substituiremos pelas letras A, E e O, respectivamente, pois são as que apresentam maior frequência na língua portuguesa, conforme a tabela dada (LOUREIRO, 2014, p. 5 e 6). É fácil escrever uma mensagem curta cuja contagem de frequência seja totalmente diferente da contagem de frequência média da língua portuguesa (MARQUES, 2013, p. 7). Por exemplo, na frase "Zuzu zoou da Zezé", a letra mais frequente é o "Z" que aparece 5 vezes em um texto de 14 letras, muito acima dos usuais 0,47%. Já o "A" aparece uma única vez, portanto, abaixo dos 14% usuais (COUTINHO, 2009, p. 11). De um modo geral, textos curtos têm maior probabilidade de se desviarem, significativamente, das frequências padrão; caso haja menos de 100 letras, a decodificação será muito difícil (MARQUES, 2013, p. 7).

A idade das trevas na Europa, também o foi para a criptografia. Durante a idade média, a criptografia era vista como magia negra, o que levou à perda de grande parte do conhecimento que existia (FIARRESGA, 2010, p. 9). Por isso, durante esse período, a Europa ainda utilizava a técnica da substituição monoalfabética (SANTOS, 2013, p. 20).

A criação da criptoanálise como ciência, a partir da definição do método de análise de frequências, deu início a uma permanente luta entre os criadores e os quebradores de códigos, o que, desde aquela época, vem beneficiando ambas as partes (SANTOS, 2013, p. 20). O surgimento do ataque de análise de frequência fez com que as cifras de substituição monoalfabéticas se tornassem obsoletas. Coube nesse momento aos criptógrafos desenvolverem uma nova cifra que se provasse imune ao ataque de análise de frequência (LOUREIRO, 2014, p. 6).

Segundo Daineze (2013), em 1411, surgem as primeiras *cifras homofônicas*. Para dificultar a análise de frequências, são introduzidos os *homófonos* e os *nulos*. Os primeiros consistiam de símbolos diferentes para representar a mesma letra e, os últimos eram colocados aleatoriamente ao longo do texto cifrado para confundir a análise de frequências do texto. Proposto por Simeone de Crema, em 1412, este código consistia em atribuir a cada letra do alfabeto, certa quantidade de símbolos, dependendo de sua frequência no alfabeto (SANTOS, 2013, p. 20). Daineze (2013) afirma que a letra "A", por exemplo, corresponde a 14% de todas as letras que aparecem num texto em português (veja Figura 6: Frequência Relativa das Letras na Língua Portuguesa), daí, deve-se criar 14 símbolos para representá-la e,

a cada vez que a letra “A” aparecer no texto original, substituímos por um dos 14 símbolos criados.

Com a descoberta do segredo da cifra de substituição monoalfabética, por meio da análise de frequências, em 1460, o italiano *Leon Battista Alberti* escreveu um ensaio no qual propunha a utilização alternada de dois ou mais alfabetos para codificar uma mensagem (SCHURMANN, 2013, p. 21). A vantagem crucial do sistema de *Alberti* é que a mesma letra do sistema original não aparece, necessariamente, como uma única letra no texto cifrado (LOUREIRO, 2014, p. 7). Alberti também foi um dos primeiros a projetar e usar um dispositivo que facilitava o processo criptográfico, este dispositivo ficou conhecido como *Disco de Alberti* (veja Figura 7: Disco de Alberti) (LOUREIRO, 2014, p. 7). Ele pegou dois discos de cobre, um maior que o outro e fixou as letras do alfabeto ao longo dos discos, colocando o disco menor em cima do maior e fixando um pino para agir como eixo. Os discos podiam ser girados independentemente, fazendo com que os dois alfabetos mudassem suas posições (SINGH, 2003, apud OLGIN, GROENWALD e FRANKE, 2011, p. 6). O disco menor poderia ser girado e, com isso, poderia ser usado para cifrar uma mensagem utilizando a cifra de César (MARQUES, 2013, p. 13 e 14).

Embora fosse um dispositivo muito básico, o disco de cifras, possibilitava o trabalho de cifragem e foi utilizado por séculos (MARQUES, 2013, p. 14). O Disco de Cifras é um misturador que pega uma letra do texto normal e a transforma em outra letra no texto cifrado (OLGIN, 2011, p. 24). Porém seu inventor sugeriu que fosse mudada a disposição do disco durante uma mensagem, o que iria gerar uma cifra polialfabética, o que dificultaria a sua decodificação, pois desse modo ele estaria mudando o modo de mistura durante a cifragem e isso tornaria a cifra difícil de ser quebrada (OLGIN, GROENWALD e FRANKE, 2011, p. 6).

Alberti não conseguiu concluir sua ideia de forma que criasse um novo sistema de criptografia completo, mas suas ideias serviram de base para a criação de um estudioso francês (SCHURMANN, 2013, p. 21).

Figura 7: Disco de Alberti
Fonte: http://www.mateureka.it/wp-content/uploads/2012/11/disco-cifrante-leon-battista-alberti.jpg

Olgin, Groenwald e Franke (2011) relatam que como as cifras de substituição monoalfabéticas eram muito simples e facilmente decifradas por criptoanalistas, através da análise de frequência de cada letra, no texto cifrado, surge a necessidade de criar novas cifras, mais elaboradas e mais difíceis de serem descobertas. Para Loureiro (2014), as *Cifras Polialfabéticas* são cifras que trabalham com vários alfabetos cifrados, sendo cada letra do texto claro substituída pela referente no alfabeto cifrado, porém sempre alternando o alfabeto cifrado.

Segundo Groenwald e Olgin (2010), a solução encontrada no século XVI, pelo diplomata francês *Blaise Vigenère* (Figura 8: Blaise Vigenère), foi uma *Cifra de Substituição Polialfabética*. *Vigenère* se inspirou nas ideias originais de Alberti e aperfeiçoou o que já havia sido desenvolvido pelo alemão *Johannes Trithemius* (1462 – 1516) e pelo italiano *Giovanni Batistta Della Porta* (1541 – 1615) (SCHURMANN, 2013, p. 21).

Figura 8: Blaise Vigenère
Fonte: https://d1u1p2xjjiahg3.cloudfront.net/6fb32fd9-e619-4a8f-9a1c-c7906d8cff50.jpg

A *Cifra de Vigenère* utiliza 26 alfabetos cifrados diferentes para codificar uma mensagem. A Tabela 5: Quadro do Quadrado de Vigenère

Fonte: Singh (2003, apud JESUS, 2013) a seguir, é conhecida como o *Quadrado de Vigenère*.

Alfabeto Normal	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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

Tabela 5: Quadro do Quadrado de Vigenère
Fonte: Singh (2003, apud JESUS, 2013)

De acordo com Olgin, Groenwald e Franke (2011), no Quadrado de Vigenère temos o alfabeto normal, seguido de 26 alfabetos cifrados, cada alfabeto tem um deslocamento de uma casa à frente no mesmo alfabeto, seguindo o princípio do Código de César. Com o auxílio dessa tabela, cada letra pode ser cifrada usando qualquer uma das 26 linhas.

Segundo Schurmann (2013), utilizando a cifra de Vigenère, podemos decodificar a mensagem recebida, desde que saibamos a palavra chave utilizada para fazer a decodificação, pois ao receber a mensagem, o decodificador terá que escrever o texto e abaixo dele será repetida a palavra chave quantas vezes forem necessárias. Junior (2013) relata que isso exige um sistema previamente combinado para a mudança entre as linhas, isto é, a palavra chave precisa ser compartilhada previamente entre o remetente e o destinatário, o que muitas vezes, era um problema, principalmente quando as pessoas não podiam se encontrar para combinar a chave.

Por exemplo, vamos cifrar a palavra: “MATEMÁTICA”, utilizando a chave: “UFOPA”.

Para codificar a mensagem, temos que escrever a palavra-chave quantas vezes for necessário (ver Tabela 6: Exemplo do uso da cifra de Vigenère), pois cada letra da palavra **UFOPA** equivale a uma letra na frase.

U	F	O	P	A	U	F	O	P	A
M	A	T	E	M	A	T	I	C	A

Tabela 6: Exemplo do uso da cifra de Vigenère
Fonte: Do Autor

Para codificar as letras da frase é necessário usar a linha correspondente à letra da palavra-chave relacionada. Para “U”, por exemplo, usaremos o alfabeto da linha 20. Assim, o primeiro “M” da frase será traduzido como “G”. Para “F”, usaremos a linha 5 e o “A” seria traduzido como “F” (veja Tabela 7: Exemplo do uso da Cifra de Vigenère).

A frase codificada ficará assim:

Palavra Chave	U	F	O	P	A	U	F	O	P	A
Texto Normal	M	A	T	E	M	A	T	I	C	A
Texto Cifrado	G	F	H	T	M	U	Y	W	R	A

Tabela 7: Exemplo do uso da Cifra de Vigenère
Fonte: Do Autor

A grande vantagem da cifra de Vigenère é que ela é imune à análise de frequência e, possui um número grande de possíveis chaves. Isso fez com que a cifra de Vigenère ficasse conhecida como *le chiffre indechiffrable* (a cifra indecifrável) (LOUREIRO, 2014, p. 8).

Segundo Costa (2014) e Jesus (2013) a cifra de Vigenère foi uma campeã em segurança, foram precisos cerca de 300 anos para ser quebrada. Mesmo sendo tão mais complexa, a cifra de Vigenère foi quebrada pelo matemático inglês Charles Babbage, por volta de 1850; e, pelo matemático alemão Friederich Kasiski que fez um estudo do padrão que a palavra chave criava ao ser repetidamente utilizada, ao longo do texto.

De acordo com Santos (2013), a técnica utilizada por Babbage para quebrar a cifra de Vigenère se resumiu em determinar o comprimento **k** da palavra chave e, depois, dividir a mensagem criptografada em **k** textos, cujas letras estão a uma distância **k** uma das outras. Após esta etapa, bastava aplicar a análise de frequência em cada um dos textos.

A quebra da cifra de Vigenère instaurou um clima de insegurança na transmissão secreta de mensagens e a idade Moderna termina da mesma forma como começou, com os criadores de códigos em busca de uma nova cifra que pudesse restabelecer a comunicação segura (SANTOS, 2013, p. 23).

2.4 A Criptografia nos Tempos Modernos

Segundo Marques (2013) o desenvolvimento da criptografia até os dias atuais foi determinado por três períodos: o *artesanal*, o *mecânico* e o *digital*. O período artesanal registra os primeiros indícios de utilização da criptografia, paralelamente ao surgimento da escrita, ocorrendo durante as idades antiga e média. No início da idade moderna, surgem os primeiros indícios do período mecânico, devido à invenção da imprensa. E o período digital surge juntamente com a invenção dos computadores e sua capacidade cada vez maior de realizar operações matemáticas que seriam impossíveis de serem feitas à mão.

Costa (2014) afirma que a quebra da cifra de Vigenère mostrou a vulnerabilidade das cifras de substituição, voltando a atenção dos criptoanalistas para outras formas de encriptação. Uma dessas formas é embaralhar o texto, ao invés de substituir as letras. Uma das maneiras de fazer isso é criptografar a mensagem por transposição. Ainda segundo Costa (2014), a forma mais simples de se fazer isso é a transposição geométrica, assim chamada por utilizar como base uma matriz retangular. O texto original é escrito dentro de uma matriz, no sentido das linhas, completando com "X" os espaços que sobram. Após, é feita a transposição da matriz. A mensagem criptografada é obtida pelo conjunto de blocos de letras formadas pelas linhas da matriz transposta.

Segundo Anton e Rorres (2001) outra maneira de superar o problema (da análise de frequências) é dividir o texto em grupos de letras e criptografar o texto comum por grupo, em vez de uma letra de cada vez. Ainda segundo os autores, um *Sistema Poligráfico* é um sistema de criptografia no qual o texto comum é dividido em conjuntos de **n** letras, cada um dos quais é substituído por um conjunto de **n** letras cifradas.

De acordo com Jesus (2013) e Anton e Rorres (2001) um dos métodos de criptografar, que utiliza essa ideia, é a chamada Cifra de Hill, que se utiliza de transformações matriciais e de um sistema poligráfico. Essa cifra recebeu esse nome, pois faz referência a *Lester S. Hill*, que introduziu esse sistema em dois artigos escritos em 1929 e 1931: *"Cryptography in the Algebraic Alphabet"* e *"Concerning Certain Linear Transformation Apparatus of Cryptography"*.

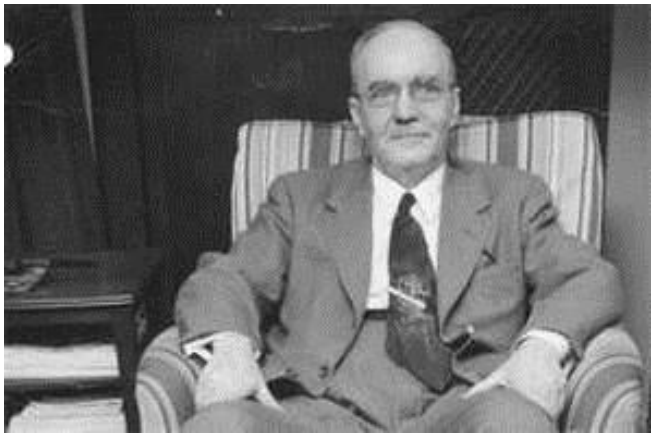


Figura 9: Lester S. Hill
Fonte: http://historyoflinearalgebra.weebly.com/uploads/1/6/5/9/16590246/842625134.jpg?298

Segundo Singh (2001 apud NETO, 2014), a primeira máquina criptográfica que se tem registro foi inventada no seculo XV pelo arquiteto italiano Leon Battista Alberti, o disco de cifras, já mencionado e descrito anteriormente. O disco de cifras foi utilizado por séculos.

De acordo com Daineze (2013), Gilbert Sandford Vernam, utilizando uma chave aleatória, inventou uma máquina de cifragem polialfabética. O surgimento do rádio como uma poderosa ferramenta de comunicação, exigia técnicas de cifragem ainda mais fortes e à prova de ataques, pois a comunicação via rádio era aberta e poderia ser facilmente inteceptada pelo inimigo (SANTOS, 2013, p. 24).

Com o século XX vieram as guerras mundiais. Para Santos (2013), nos preparativos para a Primeira Guerra Mundial, todos os países envolvidos contavam com o poder de comunicação do rádio e com a incerteza da comunicação segura.

Apesar de muito simples, criptografia por transposição serviu de base para outro algoritmo, que foi utilizado durante a Primeira Guerra Mundial (COSTA, 2014, p. 23). No final da Primera Guerra Mundial, em março de 1918, o exército alemão inventou e usou a Cifra ADFGVX, que era simultâneamente de substituição e transposição; que foi quebrada em 02 de junho do mesmo ano, pelo tenente francês Georges Painvin (FIARRESGA, 2010, p. 18).

Segundo Fiarresga (2010), a primeira parte da construção desta cifra era algo semelhante à cifra de Políbio; pois consistia numa tabela de 7x7, onde na primeira linha e na primeira coluna colocamos, respectivamente, as letras A, D, F, G, V e X, nos espaços restantes colocamos, de forma aleatória, as 26 letras e os 10 algarismos (ver Tabela 8: Cifra ADFGVX), o que nos dá 36! chaves diferentes para construir a matriz. É claro que receptor e emissor tinham que partilhar a mesma tabela.

	A	D	F	G	V	X
A	Q	S	9	X	2	A
D	V	0	Y	W	P	5
F	7	C	F	N	3	M
G	T	Z	O	6	R	B
V	U	4	J	H	K	1
X	8	L	D	G	I	E

Tabela 8: Cifra ADFGVX
Fonte: (FIARRESGA, 2010)

Ainda segundo o autor, as letras A, D, F, G, V e X foram escolhidas porque as mensagens eram transmitidas em Código Morse, e essas letras neste código são bastante diferentes, o que minimizava os erros quando a mensagem era transmitida. Cada letra ou algarismo era substituída por duas letras, de acordo com a posição que ocupasse na tabela. Por exemplo, a mensagem “PROFMAT” ficaria: DVGVGFFFFXAXGA.

De acordo com Costa (2014), a segunda etapa consistia em escolher uma palavra chave, que poderia ter qualquer tamanho, mas sem letras repetidas. Escolhemos, por exemplo, UFOPA (ver Tabela 9: Mensagem Escrita Usando a Palavra Chave). Montava-se uma tabela com as letras da palavra chave na primeira linha e, completava-se a tabela com a mensagem cifrada, uma letra para cada célula.

U	F	O	P	A
D	V	G	V	G
F	F	F	F	X
A	X	G	A	

Tabela 9: Mensagem Escrita Usando a Palavra Chave
Fonte: Do Autor

A tabela deveria ser organizada de tal forma que as letras da palavra chave ficassem em ordem alfabética, consequentemente as letras da mensagem mudavam de posição (vide Tabela 10: Tabela 9 Ordenada), era por esta nova ordem que as mensagens eram enviadas.

A	F	O	P	U
G	V	G	V	D
X	F	F	F	F
	X	G	A	A

Tabela 10: Tabela 9 Ordenada
Fonte: Do Autor

Santos (2013) relata que, impulsionada pela invenção do telégrafo e do rádio, o auge do período mecânico ocorre com o surgimento de máquinas de cifragem utilizadas durante a Segunda Guerra Mundial, dentre as quais podemos destacar a máquina alemã *Enigma*. A Revolução Industrial criou no homem a paixão pelas máquinas e a esperança de substituição do cansativo trbalho manual pelo mecânico.

2.4.1 A Criptografia na Segunda Guerra Mundial

Segundo Neto (2014), em 1918, os inventores alemães *Arthur Scherbius* e *Richard Ritter* fundaram uma empresa, a *Scherbius & Ritter*. Um de seus projetos era substituir os sistemas de criptografia, que eram muito básicos, utilizados na Primeira Guerra Mundial.

Patentearam a invenção de uma máquina de cifra mecânica, conhecida popularmente como *Enigma* (veja Figura 10: A Máquina Enigma).

Figura 10: A Máquina Enigma
Fonte: http://cdn.wp.clicrbs.com.br/plural/files/2015/02/maquina-enigma-museo-bletch.jpg

Ainda de acordo com o autor, a *Scherbius & Ritter* produziu e vendeu a *Enigma* em larga escala em 1925, pelo fato de as autoridades alemães acreditarem na segurança absoluta que ela proporcionava. Trinta mil máquinas foram vendidas e utilizadas, nas duas décadas seguintes pelo exército alemão. A *Enigma* era extremamente forte e, por treze anos, os criptoanalistas franceses e britânicos acreditavam que mensagens cifradas por ela eram impossíveis de serem quebradas, sem o conhecimento da chave.

Fiarresga (2010) afirma que a máquina *Enigma*, utilizada pelos alemães, era formada pelos seguintes componentes: um teclado, uma unidade de cifragem e um painel de visionamento. O operador para cifrar uma mensagem, utilizava o teclado para introduzir as letras do texto simples uma a uma; na unidade de cifragem, cada letra era transformada numa outra; a letra transformada era então comunicada ao operador através do painel de visionamento, onde era acessa a lâmpada correspondente (veja Figura 11: Componentes da Máquina Enigma).

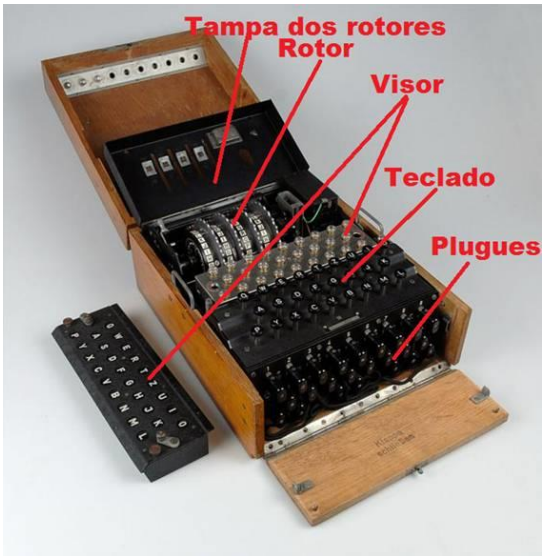


Figura 11: Componentes da Máquina Enigma
Fonte: http://videotuto.net.br/wp-content/uploads/2013/12/image002.jpg

O mesmo autor relata que a unidade de cifragem era composta por três cilindros móveis (Figura 12: Cilindro da Máquina Enigma), que podiam alternar a sua posição dentro da máquina, e um fixo, que se chamava espelho. Cada um dos cilindros continha as 26 letras do alfabeto. Entre o teclado e o primeiro cilindro existia um painel de ligação, que permitia a troca de seis pares de letras das 26 do alfabeto, o que elevava bastante o número de chaves que a máquina podia utilizar. Para cada letra cifrada, o primeiro cilindro rodava um sexto, sempre no sentido horário, quando dava uma volta completa; o segundo cilindro rodava também um sexto, após seis voltas do primeiro cilindro, o segundo dava uma volta completa; e o terceiro, rodava um sexto. Ou seja, para cada seis letras cifradas, o segundo cilindro se movia; e por 36 letras, movia-se o terceiro, o que permitia o uso de 17576 alfabetos de cifras diferentes.

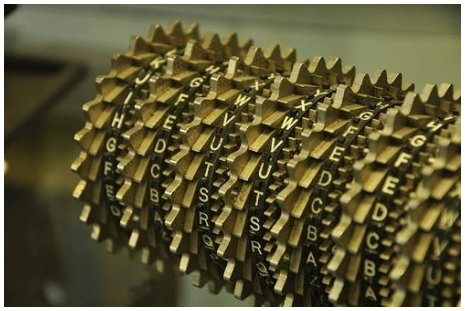


Figura 12: Cilindro da Máquina Enigma
Fonte: http://www.wikinoticia.com/images2//s1.alt1040.com/files/2012/04/Enigma.jpg

O autor ainda afirma que não era só no número de alfabetos de cifras que a enigma era forte, seu número de chaves era muito grande. O seu verdadeiro número de chaves pode ser calculado da seguinte maneira:

Para começar, os cilindros podiam permutar entre si, como eram 3, temos 3! = 6;

Cada um dos 3 cilindros podia ser regulado de 26 maneiras diferentes, o que dá 26^3 = 17576;

No painel de comunicação, podiam-se trocar 6 pares de letras, a partir das 26 letras do alfabeto, o que pode ser feito de $\frac{(26.25).(24.23).(22.21).(20.19).(18.17).(16.15)}{2^6.6!} = 100391791500$ maneiras diferentes;

Por fim, o número de chaves era dado por: 17576 . 6 . 100391791500 = 1058691676442400.

A colocação dos cilindros, a sua regulação inicial e o conhecimento da troca dos seis pares de letras determinavam a chave a usar.

Olgin, Groenwald e Franke (2011) afirmam que para decifrar uma mensagem da *Enigma* o destinatário precisaria ter outra Enigma e uma cópia do livro de códigos, contendo o ajuste inicial dos misturadores para cada dia. A Enigma é conhecida como o mais terrível sistema criptográfico da história, por ter sido utilizada pelos alemães durante a Segunda Guerra Mundial, dando a eles o mais seguro sistema de criptografia do mundo.

Ainda para os mesmos autores, durante anos os alemães acreditaram que a *Enigma* era indecifrável até *Hans-Thilo Schmitdt* vender informações sobre a máquina para as potências estrangeiras, prejudicando assim a segurança da Alemanha, pois a partir das informações dadas por ele, era possível criar uma réplica da *Enigma*. Essas informações, porém, não eram suficientes para decodificar as mensagens da máquina, pois era necessário saber o ajuste inicial dela.

Santos (2013) relata que mesmo com seu alto nível de complexidade, as mensagens da Enigma começaram a ser decifradas frequentemente. A quebra do código da máquina Enigma foi um dos maiores triunfos criptoanalíticos de todos os tempos, num experimento que envolveu o esforço conjunto de poloneses, franceses e ingleses, em plena guerra.

O autor ainda afirma que o trabalho começou com o matemático polonês *Marian Rejewski*, que se baseou em textos cifrados interceptados e em uma lista de três meses de chaves diárias, obtidas através do serviço de espionagem francês. As contribuições de Rejewski foram muito importantes, apesar de não conclusivas. Seus esforços foram concluidos pela equipe inglesa liderada por *Alan Turing*, *Gordon Welchman* e outros, em Bletchley Park, na Inglaterra.

Ainda segundo Santos (2013), para quebrar o código da Enigma, Turing e seus colaboradores desenvolveram dois tipos de máquinas: a primeira foi denominada *Bomba* e a segunda, *Colossus*. A grande dificuldade encontrada pela equipe de Turing ocorreu em função

de que os alemães mudavam regularmente a configuração da Enigma. Além das chaves que tinham validade mensal, mudanças contínuas foram implementadas, com destaque para o acréscimo de dois misturadores, incrementando, de modo impressionante, o número de chaves possíveis.

Segundo Olgin, Groenwald e Franke (2011) e Jesus (2013), em 1943, foi projetado o *Colossus* (veja Figura 13: A Máquina Colossus), um gigantesco computador, projetado especialmente para decifrar mensagens cifradas pela Enigma. Ele possuía uma dimensão enorme e funcionava por meio de relés, que chegavam a processar cerca de 5 mil caracteres por segundo, através de um sistema fotoelétrico. Todas as mensagens eram comparadas às mensagens geradas pelas chaves criptográficas do Colossus, para revelar a configuração da máquina usada pelos alemães. A Colossus deu início a uma era moderna da criptografia, onde os computadores eram programados com chaves de codificação muito mais complexas do que as utilizadas pela Enigma, essa nova técnica de criptografia era de uso exclusivo do governo e de militares para guardar informações.

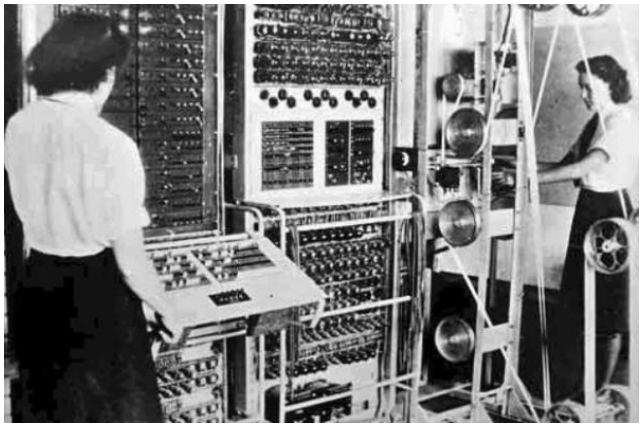


Figura 13: A Máquina Colossus
Fonte: http://img.ibxk.com.br/2013/6/materias/9119619556173414.jpg?w=1040&h=585&mode=crop

A quebra da criptografia utilizada pelos nazistas deu aos aliados uma vantagem fundamental, que, de acordo com historiadores, encurtou a guerra em mais de dois anos, salvando muitas vidas (NETO, 2014, p. 21).

3 A CRIPTOGRAFIA E OS COMPUTADORES

Gomes (2014) afirma que, antes do século XX, a criptoanálise podia ser feita com papel e caneta, mas as inovações como as máquinas baseadas em rotores durante as grandes

guerras mundiais tornaram essa tarefa extremamente complicada. Ainda assim foi possível ao intelecto de Alan Turing e sua equipe, cujo trabalho assentou as bases para a computação, quebrar o código nazista. O computador pode efetuar uma quantidade de cálculos que seria impossível de realizar a mão por uma pessoa.

Segundo Fiarresga (2010), em meados do século XX, o aparecimento do computador veio revolucionar o mundo da criptografia. A grande capacidade do computador para cifrar mensagens, aliada ao fato do computador modificar números e não letras do alfabeto, trouxe vários problemas ao mundo da criptografia. Com a utilização crescente de computadores por parte das empresas e a necessidade do uso da criptografia como medida de segurança, surgiu a necessidade de uma padronização, de modo, que as empresas pudessem trocar mensagens de uma forma segura e eficiente.

Para Olgin, Groenwald e Franke (2011) os computadores utilizavam criptografias complexas, mas não apresentavam a segurança necessária para não serem invadidos por pessoas que não deveriam ter acesso aos códigos de encriptação contidos nele. Para solucionar este problema foram criados dois algoritmos de codificação o DES (sistema de chave secreta) e RSA (sistema de chave pública).

Sobre o assunto, Santos (2013) afirma que com o desenvolvimento e aperfeiçoamento dos computadores, a incrível capacidade de realizar mais de um milhão de operações por segundo e a necessidade de uso da criptografia pelo comércio e bancos, os algoritmos criptográficos passam a ser de conhecimento público e o segredo a residir exclusivamente na chave.

3.1 Criptografia Simétrica

Gomes (2014) relata que durante muito tempo a criptografia foi feita usando-se chaves simétricas, que é o uso da mesma chave, tanto para codificar quanto para decodificar (decifrar) a mensagem, de certa forma, é um problema, pois há dificuldade na maneira de comunicar essa chave ou no gerenciamento de múltiplas chaves em comunicação com um número elevado de pessoas.

Para Marques (2013) a Criptografia Simétrica (ou de chave privada) transforma um texto claro em um texto cifrado, usando uma chave secreta e um algoritmo de criptografia. A partir da mesma chave e com o auxílio de um algoritmo de decriptografia, o texto claro pode ser recuperado, usando-se o texto cifrado como ponto de partida. Também conhecida como

secret-key ou symmetric-key encryption. Esta chave pode ser uma palavra, frase ou uma sequência aleatória de números e/ou símbolos. O tamanho da chave é medido em bits e, via de regra, quanto maior for a chave, mais seguro será o documento cifrado (veja Figura 14: Esquema Simplificado do Algoritmo de Chave Simétrica).

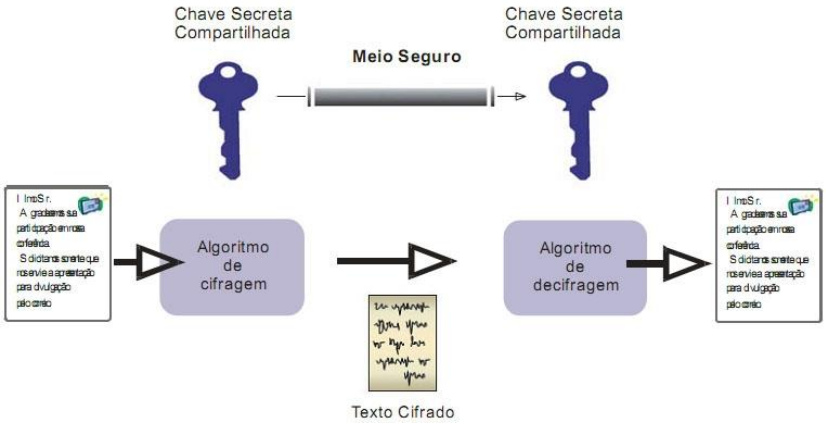


Figura 14: Esquema Simplificado do Algoritmo de Chave Simétrica
Fonte: http://www.gta.ufrj.br/grad/07_2/delio/NotesImages/Topic12NotesImage3.jpg

Ainda para Marques (2013), para um remetente e um destinatáio se comunicarem utilizando este método, eles devem concordar quanto a chave e devem manter isso em segredo. Estando eles em lugares diferentes, deverão se comunicar de algum jeito: encontrar-se, telefone, mensagem de texto, e-mail, um mensageiro; enfim, algum meio de comunicação que eles considerem seguro. Como fazer com que o destinatário receba a chave sem alguém interceptá-la? Isto se tornou um problema fundamental na informática, conhecido como "o problema da troca de chaves".

Santos (2013) afirma que a operação de chave simétrica é mais simples, pois pode existir uma única chave entre as operações. A chave, na prática, representa um segredo, partilhado entre duas ou mais partes, que podem ser usadas para manter um canal confidencial de informação. Usa-se uma única chave, partilhada por ambos os interlocutores, na premissa de que esta é conhecida apenas por eles.

De acordo com Oliveira (2006, apud MARQUES, 2013) e Santos (2013), os principais algoritmos de chave privada são: DES, 3-DES, AES e IDEA.

3.1.1 DES

Segundo Gomes (2014), na década de 1960, o alemão Horst Feistel (1915 – 1990), à frente de uma equipe de pesquisa da IBM, traz a público a cifra Lúcifer, uma cifra de bloco

cuja versão DTD-1 passa a ser usada nos caixas eletrônicos na década de 1970. O governo americano analisa a cifra Lúcifer em 1976, com a ajuda da NSA (National Security Agency, em português: Agencia Nacional de Segurança) e do NBS (National Bureau of Standards, em português: Escritório Nacional de Padrões), eles sugerem algumas modificações e passam a usá-la como padrão de encriptação, agora conhecida como DES (Data Encryptation Standard, em português: Padrão de Encriptação de Dados).

Para Olgin, Groenwald e Franke (2011) Lúcifer era tão poderoso que oferecia a possibilidade de um padrão de cifragem além das capacidades de quebra de códigos da NSA. Como a NSA não iria querer um padrão de cifragem que ela não poderia quebrar, então limitou o número de chaves do sistema Lúcifer, de modo que ele oferecesse segurança à comunidade civil e que a NSA seria capaz de decodificar. A versão do sistema Lúcifer com a chave limitada foi oficialmente adotada em 23 de novembro de 1976 e batizada como Padrão de Cifragem de Dados (DES – Data Encryption Standard).

De acordo com Olgin, Groenwald e Franke (2011), a DES é um algoritmo de criptografia em blocos, composto da substituição de caracteres em blocos de 64 bits, utilizando uma chave de 56 bits. Sua estrutura é composta de 16 estágios de criptografia, executando, durante todo o processo, séries de transposições e substituições de caracteres, bem como, a recombinação de blocos.

Ainda segundo Olgin, Groenwald e Franke (2011), a adoção da DES resolveu um problema de padronização, encorajando as empresas a utilizarem a criptografia para sua segurança. A DES era suficientemente forte para garantir a segurança contra ataques de rivais comerciais, pois era impossível para uma empresa com um computador civil, quebrar uma mensagem cifrada com a DES, porque o número de chaves possíveis era suficientemente grande. O problema do algoritmo DES é a distribuição de chaves, pois a chave de codificação é a mesma de decodificação. O DES não se baseia em manter o segredo do seu algoritmo de codificação, mas no segredo da chave usada para codificar uma mensagem específica.

De acordo com os mesmos autores, a tecnologia DES tem sido utilizada em vários produtos comerciais e é o algoritmo de criptografia escolhido pelos usuários comerciais. Várias companhias utilizam o DES, dentre elas estão: a General Eletric, a IBM e a Motorola.

3.1.2 3-DES

Segundo Gomes (2014), em 1999, o padrão DES de 56 bits foi, quebrado por um computador chamado Deep Crack, depois de trabalhar por 22 horas e 15 minutos. Em resposta o governo americano adota o 3-DES, a aplicação tripla do DES com chaves de 64 bits.

Para Santos (2013), o 3-DES é uma simples variação do DES, utilizando-o em 3 ciframentos sucessivos, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.

3.1.3 AES

Segundo Marques (2013), o Advanced Encryption Standard (AES) é uma cifra de bloco, anunciado pelo NIST (National Institute of Standards and Technology, ou, Instituto Nacional de Padrões e Tecnologia) em 2003, fruto de concurso para escolha de um novo algoritmo de chave simétrica para proteger informações do governo federal, sendo adotado como padrão oficial pelo governo dos Estados Unidos, é um dos algoritmos mais populares, desde 2006, usado para criptografia de chave simétrica, sendo considerado como padrão substituto do DES. O AES tem um tamanho de bloco fixo de 128 bits e uma chave de tamanho de 128, 192 ou 256 bits. Ele é rápido tanto em software quanto em hardware, é relativamente fácil de executar e requer pouca memória.

3.1.4 IDEA

Para Marques (2013) e Santos (2013), o International Data Encryption Algorithm (IDEA) foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES. O IDEA é usado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo.

Fiarresga (2010) afirma que o IDEA, como ficou conhecido, foi uma proposta para um novo padrão de encriptação de bloco, que viria a substitui o DES. O IDEA utiliza uma

chave de 128 bits e emprega operações adequadas para a maioria dos computadores, tornando as implementações do software mais eficientes.

Marques (2013) ainda afirma que outros algoritmos de chave privada são Blowfish, Twofish, RC4 e CAST.

Fiarresga (2010) afirma que o problema da distribuição de chave continuava em aberto. A melhor forma de emissor e receptor trocarem uma chave continua sendo na base da confiança, o que gerava grandes encargos para governos, empresas e bancos.

3.2 Criptografia Assimétrica

De acordo com Gomes (2014), na criptografia a natureza das chaves passa a se dar de duas formas: simétricas ou assimétricas. O uso de chaves assimétricas, em que o emissário e o destinatário da mensagem possuem chaves diferentes, com uma operando de forma inversa à outra, resolveu os problemas de distribuição e gerenciamento de chaves.

Segundo Marques (2013), a Criptografia Assimétrica (ou de chave pública) transforma um texto claro em texto cifrado usando uma de duas chaves e um algoritmo de criptografia. Usando a outra chave associada e um algoritmo de decriptografia, o texto claro é recuperado, a partir do texto cifrado. A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada deverá ficar em poder de apenas cada titular (veja Figura 15: Esquema Simplificado do Algoritmo de Chave Assimétrica).

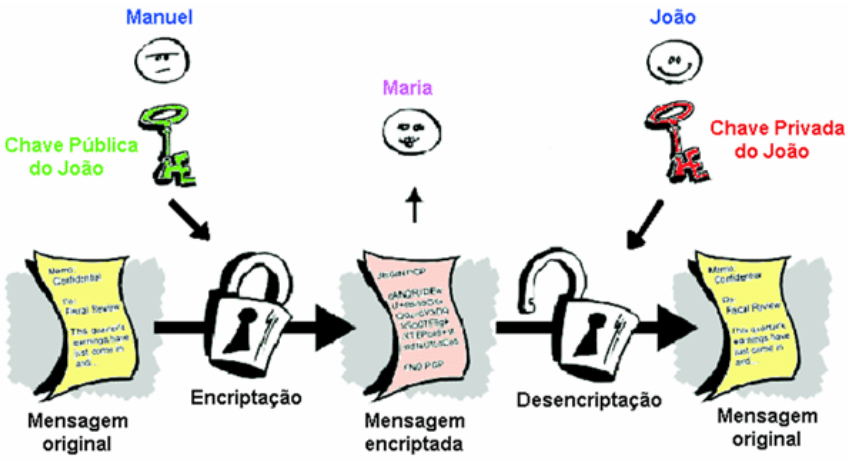


Figura 15: Esquema Simplificado do Algoritmo de Chave Assimétrica
Fonte: http://www.dm.ufscar.br/profs/caetano/iae2004/G6/images/assimetrica.gif

Para Marques (2013) a principal vantagem deste método é a sua segurança, pois não é preciso (nem se deve) compartilhar a chave privada. Deve-se destacar que na criptografia assimétrica, o tempo de processamento de mensagens é muitas vezes maior do que na criptografia simétrica, dando maior dificuldade para o criptoanalista que deseja decifrar a mensagem.

De acordo com Faleiros (2011, apud JESUS, 2013), em 1976, Bailey Whitfield Diffie e Martin Edward Hellman publicaram um artigo denominado "New Directions in Cryptography", no volume 22 da revista IEE Transactions on Information Theory. Neste artigo descreveram o primerio método para trocar uma chave secreta entre dois agentes, usando um canal público. O trabalho de Diffie e Hellman foi um marco na criptografia, e abriu as portas para a criptogafia de Chave Pública.

Para Jesus (2013) até meados da década de 1970, a transmissão de mensagem fazia uso exclusivo de chaves privadas para criptografar e decodificar mensagens. Em 1976, uma mudança de paradigma aconteceu quando Diffie e Hellman propuseram o uso de chaves públicas. Santos (2013) completa afirmando que, o Diffie Hellman Key Exchange, como ficou conhecido o algoritmo, tornou possível a comunicação por criptografia sem a necessidade de compartilhamento antecipado de uma chave secreta comum. Uma abordagem da comunicação segura radicalmente diferente e de uma elegância que levou ao desenvolvimento dos atuais sistemas de Criptografia de Chaves Públicas.

Segundo Couto (2008, apud GOMES, 2014), os pesquisadores Ronald L. Rivest, Adi Shamir e Leonard M. Adleman atendem à sugestão de Diffie e Hellman e apresentam, em um artigo de 1977, a cifra RSA, uma cifra de chave pública, que era tanto para processo de criptografia quanto para assinatura digital.

Coutinho (2009) afirma que o mais conhecido dos métodos de criptografia de chaves públicas é o RSA. Os inventores trabalhavam no MIT (Massachussets Institute of Technology), quando desenvolveram esse método. As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais.

Para Santos (2013), o uso de criptografia de chave pública é conceitualmente simples, mas apresenta duas preocupações. A primeira, diz respeito ao conhecimento público da chave e do algoritmo de criptografia. Fica claro que, para a criptografia de chave pública funcionar, a escolha de chaves e de códigos de criptografia/decriptografia deve ser feita de tal forma que seja praticamente impossível para um intruso determinar a chave privada do destinatário. A segunda preocupação reside no envio da mensagem cifrada, como a chave

criptográfica é pública, qualquer um pode enviar uma mensagem cifrada para o destinatário. Neste caso, faz-se necessário o uso de uma assinatura digital, que visa garantir a autenticidade de quem envia a mensagem, associada à integridade de seu conteúdo, vinculando um remetente específico à mensagem.

Segundo Oliveira (2006, apud MARQUES, 2013) e Santos (2013), os principais algoritmos de chave assimétrica são: RSA, ElGamal, Diffie-Hellman e Curvas Elípticas.

3.2.1 RSA

Oliveira (2006, apud MARQUES, 2013) e Santos (2013) afirmam que o RSA, atualmente, é o algoritmo assimétrico (de chave pública) mais amplamente usado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecida até o momento. O RSA utiliza números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, e na dificuldade de recuperar os dois primos a partir do terceiro número (fatoração). Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e "bem escolhido", então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA, baseia-se na dificuldade de fatoração de números grandes.

3.2.2 ElGamal

Segundo Oliveira (2006, apud MARQUES, 2013) e Santos (2013), o ElGamal, é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema de fatoração.

3.2.3 Diffie-Hellman

De acordo com Oliveira (2006, apud MARQUES, 2013) e Santos (2013), o algoritmo Diffie-Hellman, também baseado no problema do logaritmo discreto, trata-se do criptossistema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás, foi introduzido pelos autores deste criptossistema em 1976. O problema deste método é que ele não permite ciframento, o sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.

3.2.4 Curvas Elípticas

Oliveira (2006, apud MARQUES, 2013) e Santos (2013) afirmam que, em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie-Hellman e o ElGamal podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública: o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

Para Santos (2013), durante algum tempo, muito se discutiu sobre a melhor forma de se criptografar: se utilizando um sistema simétrico ou assimétrico. Na realidade, existem vantagens e desvantagens em cada sistema que, dependendo do contexto e das condições, fazem com que a escolha do melhor sistema possa variar.

Segundo Fiarresga (2010), durante os anos 1990, aparecem alguns trabalhos com computadores quânticos e criptografia quântica. Na mesma época, a biometria é aplicada na autenticação. Ainda segundo o autor, os primeiros ensaios sobre criptografia quântica são publicados por Charles H. Benett e Gilles Brassard, relatando o uso de fótons para transmitir

um fluxo de bits. Para Santos (2013), em um computador quântico, a velocidade será muito maior do que no mais moderno dos computadores de nossa época. No momento, a pesquisa e o desenvolvimento de computadores quânticos ainda é incipiente e guardada em segredo, mas quando esta tecnologia se tornar realidade, novos desafios darão continuidade a esta rica história da criptografia.

4 METODOLOGIA DA INVESTIGAÇÃO

Este capítulo é destinado a especificar quais foram as metodologias da pesquisa utilizadas neste trabalho e como elas foram utilizadas dentro do mesmo.

Nossa hipótese foi que relacionar os conteúdos do Ensino Médio e as situações-problemas à teoria da Criptografia, bem como uma revisão de sua história, poderia despertar um maior interesse pelo assunto e, consequentemente uma maior compreensão dos conteúdos associados.

O grande fator problematizador desta pesquisa foi como desenvolver uma sequência didática, para ser aplicada no segundo ano do Ensino Médio, que apresentasse a Matemática como uma ferramenta que pudesse ser amplamente aplicada à codificação das transações e comunicações humanas, ou seja, à Criptografia. Uma vez desenvolvida esta sequência didática, ela seria atrativa aos alunos de uma forma que prendesse a atenção e os instigassem a aprender os conteúdos matemáticos associados? Em busca de respostas, procuramos referências de alguns autores que já trabalharam de forma semelhante e, encontramos algumas citações interessantes.

Para Groenwald e Franke (2008), o tema Criptografia permite interligar os conteúdos matemáticos às situações do mundo real e ajuda a desenvolver, nos alunos, habilidades e competências na criação de estratégias para a resolução de problemas e, autonomia durante o processo de aprendizagem, com isso, tornando-os mais autoconfiantes e concentrados na realização das atividades.

Sobre o assunto Groenwald e Olgin (2011) afirmam que, nesse contexto, pode-se perceber que a Criptografia possibilita o desenvolvimento de atividades didáticas, que podem ser desenvolvidas no Ensino Médio, que levem os alunos a aprimorarem seus conhecimentos.

Cantoral et. al. (2000, apud GROENWALD e OLGIN, 2011), afirmam que este tema pode ser um recurso que permitirá ao professor desenvolver atividades didáticas que proporcionem aulas que despertem a atenção e o interesse dos alunos para os conteúdos trabalhados em sala de aula.

O uso da calculadora foi implementado com o objetivo de facilitar a resolução de cálculos longos, maximizando o tempo dedicado a elaboração e discussão de estratégias de resoluções, entre os alunos de cada grupo. Evitando, dessa foma, que as resoluções das atividades se tornasem demoradas e cansativas. Na mesma linha de raciocínio, Olgin (2011) afirma que as calculadoras possibilitam que o estudante dedique maior concentração às

estratégias para a resolução de problemas, não desperdiçando tempo com cálculos longos e repetitivos, pois esse não é o objetivo das atividades propostas pelo professor.

Após observarmos as impressões de outros autores, restou-nos seguir adiante com nosso intento. Precisávamos escolher uma metodologia didática que pudesse conciliar, ao mesmo tempo, uma boa ferramenta para avaliar procedimentos didáticos mais próximos do cotidiano de sala de aula e, que não avaliasse o desempenho particular do aluno e sim o processo como um todo. A solução foi encontrada quando conhecemos a Engenharia Didática, que será descrita de forma mais detalhada a seguir.

4.1 Metodologia Científica: A Engenharia Didática

Neste trabalho, a metodologia de pesquisa adotada foi a Engenharia Didática que, de acordo com as ideias de Oliveira (2013) e Carneiro (2005), é uma metodologia de pesquisa e teoria educacional que surgiu na França no início dos anos 80 no campo específico da Didática da Matemática. O termo Engenharia Didática também pode ser usado para designar a aplicação planejada de uma sequência didática (termo usado para definir um procedimento encadeado de passos, uma espécie de roteiro, ou etapas ligadas ente si para tornar mais eficiente o processo de aprendizagem) com um grupo de alunos.

Segundo Artigue (1988, apud ALMOULOUD e SILVA, 2012) e Carneiro (2005), o termo “Engenharia Didática” foi concebido para o trabalho didático semelhante ao realizado por um engenheiro que, para realizar um projeto, se baseia nos conhecimentos científicos de sua área, submete-se ao controle de tipo científico, mas, também, necessita de trabalhar objetos menos precisos que os científicos, problemas práticos para os quais não existe teoria prévia, nesses momentos, faz-se necessária a construção de soluções.

4.1.1 Principais Características

Almouloud e Silva (2012) e Brum (2013) relatam que a Engenharia Didática é uma metodologia de pesquisa suscetível de fazer aparecer fenômenos didáticos em condições mais próximas possíveis do funcionamento de uma sala de aula. Nesse contexto, Almouloud e Coutinho (2008) afirmam que a Engenharia Didática, vista como metodologia de pesquisa, caracteriza-se, primeiramente, por um esquema experimental baseado em “realizações

didáticas" em sala de aula, isto é, na concepção, realização, observação e análise de uma sequência de ensino. Também se caracteriza como pesquisa experimental pelo registro em que se situa e modo de validação que lhe são associados: a comparação entre *análise a priori* e *análise a posteriori*. Esse tipo de validação é uma das singularidades dessa metodologia, por ser feita internamente, sem a necessidade de aplicação de um pré-teste ou de um pós-teste.

Berenguer (2010) e Pantoja e Silva (2012) afirmam que a Engenharia Didática é uma das abordagens tratadas na Didática das Ciências Exatas que se caracteriza como uma forma particular de organizar os procedimentos metodológicos de pesquisas desenvolvidas no contexto de sala de aula. Para se desenvolver uma pesquisa tendo como princípio metodológico a engenharia didática, articula-se a construção do saber matemático a uma prática reflexiva investigativa diante de uma sequência didática experimental.

No entendimento de Berenguer (2010), a Engenharia Didática pode ser tanto uma metodologia de pesquisa quanto uma sequência de aula(s) concebida(s), elaborada(s) e articulada(s) no tempo, de forma coerente, por um professor/engenheiro para realizar um projeto de aprendizagem para uma certa população de alunos. Douady (1993, apud BERENGUER, 2010) completa que, no transcorrer das trocas entre professor e alunos, o projeto evolui sob as reações dos alunos e em função das escolhas e decisões do professor. Nesse contexto vejamos o que nos diz Carneiro (2005):

> "A Engenharia Didática foi criada para atender a duas questões: das relações entre pesquisa e ação no sistema de ensino; do lugar reservado para as realizações didáticas entre as metodologias de pesquisa. É uma expressão com duplo sentido. Designa produções para o ensino, derivadas de resultados de pesquisas, e também designa uma específica metodologia de pesquisa baseada em experiências de sala de aula" (CARNEIRO, 2005, p. 4).

Para Pommer (2013) e Brum (2013), a Engenharia Didática se enquadra melhor como pesquisa qualitativa, que inicialmente, buscou estudar problemas relacionados à aprendizagem de conceitos específicos da Matemática: diagnóstico de concepções, dificuldades e obstáculos, compreender os níveis de desenvolvimento das estratégias dos alunos, a aprendizagem, introdução e construção de conhecimentos específicos, a formação de professores, explicitar a relação entre temas da Matemática e outras áreas de conhecimento, dentre outras.

De acordo com Brousseau (1982, apud BERENGUER, 2010) existem três tipos de obstáculos a serem considerados:

Epistemológico – são inerentes ao próprio saber, constitutivos do próprio conhecimento. Podem ser percebidos nas dificuldades que os próprios matemáticos encontraram na história e por isso “não podemos escapar deles e nem deixá-los escapar”.

Didático – são os que dependem da escolha de um projeto do sistema educacional, ou seja, são as dificuldades criadas pela escola, através da estratégia de ensino escolhida que provoca, posteriormente, obstáculos ao desenvolvimento da conceituação.

Ontogênico – origina-se de limitações do sujeito em um dado momento do seu desenvolvimento mental. Normalmente surgem quando a aprendizagem está muito deslocada em relação à maturidade conceitual do sujeito.

4.1.2 Fases da Engenharia Didática

Segundo vários autores, dentre eles Almouloud e Coutinho (2008), Almouloud e Silva (2012), Brum (2013), Gomez (2008), Pivatto e Schuhmacher (2013), Souza (2013) e Souza e Cordeiro (2005), Carneiro (2005), Berenguer (2010), Oliveira (2013) e Pommer (2013), pode-se dividir a Engenharia Didática em quatro fases metodológicas: a das *análises preliminares*, a da *concepção e análise a priori das situações didáticas*, a da *experimentação* e a da *análise a posteriori e validação*. Para Artigue (1988, apud SOUZA, 2013) cada uma dessas fases é retomada e aprofundada ao longo do trabalho de pesquisa, em função das necessidades emergentes.

Figura 16: Etapas da Engenharia Didática
Fonte: (BRUM, 2013)

De acordo com Artigue (1988, apud SOUZA e CORDEIRO 2005), a primeira fase, a fase das *análises preliminares*, está apoiada em um referencial teórico já obtido e analisa como se encaminha determinado conhecimento no estudante, como se dá o ensino atual em relação àquele conhecimento, as concepções dos alunos, as dificuldades e obstáculos que marcam a evolução do conteúdo a ser estudado. Já para Pivatto e Schuhmacher (2013) nessa fase é realizada a análise do objeto em estudo, ou seja, é feito um referencial teórico que irá fundamentar o projeto. O educador deve levar em consideração as contribuições empíricas, concepções do aprendiz e compreender as condições nas quais será exposta a experiência. Também deve ser realizada uma análise geral quanto aos aspectos histórico-epistemológicos dos assuntos a serem trabalhados e dos efeitos por eles provocados, da concepção, das dificuldades e obstáculos encontrados pelos alunos dentro deste contexto de ensino. Oliveira (2013) cita os passos que esta fase deve compreender, a saber: análise epistemológica dos conteúdos de ensino; análise do ensino usual e os seus efeitos; análise das concepções dos estudantes, dificuldades e obstáculos que caracterizam o desenvolvimento delas; análise do campo de limites no qual a produção didática efetivamente ocorrerá; levar em conta os objetivos específicos da pesquisa.

Segundo Artigue (1988, apud SOUZA e CORDEIRO, 2005), a segunda fase, a fase da *concepção e análise a priori* das situações didáticas, é aquela na qual o pesquisador

definirá as variáveis que estarão sob controle. “Comporta uma parte descritiva e outra preditiva”, onde o comportamento esperado do aluno é o foco principal da análise. De acordo com Artigue (1988, apud ALMOULOUD e COUTINHO, 2008) essas variáveis podem ser *macro-didáticas* ou *globais*, as quais se referem à organização geral da engenharia, ou *micro-diáticas* ou *locais*, que se referem à organização de uma fase da engenharia. Por outro lado Machado (2002, apud BRUM, 2013) comenta que a pesquisa delimita as variáveis de comando, que são as variáveis locais ou globais pertinentes ao sistema didático (professor/aluno/saber) que podem ser consideradas pelo professor/pesquisador para que sejam abordadas as várias sessões ou fases de uma Engenharia Didática. Ainda na fase de análise a priori, Berenguer (2010) relata que o pesquisador deve se preocupar em descrever as características da situação didática, verificar as possibilidades de ação dos alunos e analisar qual seria o comportamento do aluno diante da situação aplicada.

A terceira fase, fase da *experimentação*, de acordo com Artigue (1988, apud SOUZA e CORDEIRO 2005), é a ida a campo para a aplicação da sequência didática com uma certa população de alunos e os registros de observações realizadas durante a mesma. Almouloud e Silva (2012) completam que, nesta fase, deve-se ter como pressupostos apresentar os objetivos e condições da realização da pesquisa e estabelecer o contrato didático. É neste momento que ocorre a aplicação da sequência didática formada por um certo número de aulas planejadas e analisadas previamente com a finalidade de observar situações de aprendizagem (PAIS, 2002 apud BERENGUER, 2010, p. 14).

Para Almouloud e Silva (2012), a quarta fase, a fase de *análise a posteriori e validação* consiste em uma análise de um conjunto de dados coletados no decurso da experimentação, como por exemplo, produção dos alunos, registro de observadores e registro em vídeo. Nessa fase, faz-se necessário sua confrontação com a análise a priori para que seja feita a validação ou não das hipóteses formuladas na investigação. Além disso, para Artigue (1988, apud SOUZA e CORDEIRO 2005), esses dados são geralmente completados por dados obtidos pela utilização de metodologias externas: questionários, entrevistas individuais ou em pequenos grupos, realizados em diversos momentos do ensino ou a partir dele. Pivatto e Schuhmacher (2013) afirmam que, dessa forma, é possível analisar se ocorrem e quais são as contribuições para a superação do problema, caracterizando a generalização que permitirá a validação interna do objetivo de pesquisa.

Após o encerramento dessas quatro fases, faz-se necessária a elaboração de um relatório final dos resultados obtidos na Engenharia Didática vivenciada em um determinado contexto escolar. Sobre esse relatório, Oliveira (2013), nos diz que:

> "[...] é necessário fazer um confronto entre as expectativas iniciais, a análise a priori, a experimentação e a análise da construção didática. E, assim procedendo, é feita a validação ou não da hipótese inicial, quanto ao planenjamento das diferentes sessões de uma Engenharia Didática para desenvolver um determinado conteúdo no contexto de uma sala de aula" (OLIVEIRA, 2013, p. 117).

4.1.3 As Principais Contribuições da Engenharia Didática Para o Ensino/Aprendizagem

O aporte da Engenharia Didática para o ensino como campo metodológico, refere-se à possibilidade de apresentar a fundamentação teórica para que o professor conheça o significado e amplie o leque de opções, formando elo entre a teoria e a prática de sala de aula (PIVATTO e SCHUHMACHER, 2013, p.5). Segundo Souza e Cordeiro (2005) as principais diferenças entre as pesquisas realizadas dentro de uma metodologia da Engenharia Didática e outras são observadas na profundidade das análises preliminares, e também no fato da validação das hipóteses realizadas sobre o problema da pesquisa serem internas, validadas no confronto entre análise a priori e a posteriori. Para Berenguer (2010), a Engenharia Didática trata de aspectos teóricos e experimentais fazendo uma relação entre a teoria e a prática, isto é, uma conexão bastante rica entre a pesquisa e a prática educativa.

Souza e Cordeiro (2005) ainda completam que, dentro desse quadro, a ida do pesquisador a campo, busca um confronto das análises iniciais com os dados sobre os procedimentos e desempenhos dos alunos, analisados posteriormente, validando (ou não) assim as hipóteses da pesquisa. Através da Engenharia Didática o professor tem a oportunidade de refletir e avaliar a sua ação educativa e é diante desse processo de reflexão que redireciona e ressignifica o trabalho que desenvolve (BERENGUER, 2010, p. 9).

Dessa forma, segundo Pivatto e Schuhmacher (2013), o trabalho do professor é:

> "[...] propor ao estudante uma situação de aprendizagem para que elabore seus conhecimentos como resposta pessoal a uma pergunta, e os faça funcionar ou os modifique como resposta às exigências do meio e não a um desejo do professor" (BROUSSEAU, 1996 apud PIVATTO e SCHUHMACHER, 2013, p. 3).

Carneiro (2005) relata que a Engenharia didática está relacionada com o movimento de valorização do professor, com a consciência de que as teorias desenvolvidas fora de sala de aula são insuficientes para captar a complexidade do sistema e para influenciar na transformação das tradições de ensino. Dessa forma, a questão consiste em afirmar a

possibilidade de agir de forma racional, tendo por base conhecimentos matemáticos e didáticos, ressaltando a importância da realização didática na sala de aula como prática de investigação.

Para Pommer (2013), no contexto de sala de aula, as atividades a serem propostas devem ser concebidas como uma situação de aprendizagem. Este fato exige do professor um mínimo de interferência, o encorajamento a ação independente dos alunos para a busca das soluções, incentivando também, o uso dos conhecimentos prévios como ferramentas.

Segundo Carneiro (2005), a teoria da Engenharia Didática pode ser vista como referencial para o desenvolvimento de produtos para o ensino, gerados na junção do conhecimento prático com o conhecimento teórico. Sobre isso, Pantoja e Silva (2012) nos relatam que:

> "[...] as práticas educativas desenvolvidas a partir de princípios da engenharia didática devem ser compreendidas como práticas de investigação. À medida em que os professores vão trabalhando os saberes escolares, estes devem ser colocados em dúvida e discutidos para que os alunos tenham consciência da complexidade dos objetos estudados. É partindo dessa abordagem metodológica que a aprendizagem se consolida, pois nela o que importa é a compreensão a respeito do conhecimento trabalhado e não o puro e simples ato de "encher" o quadro de matéria que deve ser copiada e decorada pelos alunos para a realização de uma penosa avaliação" (PANTOJA e SILVA, 2012, p. 7).

Para um maior entendimento da teoria da Engenharia Didática, indicamos a leitura dos textos citados neste capítulo.

5 ATIVIDADES

As atividades foram realizadas em grupos de 4 ou 5 alunos, para que haja divisão de tarefas e participação de todos. Deixaremos que a montagem dos grupos, bem como a divisão de tarefas e o papel de cada membro sejam decididos pelos próprios alunos. Preconizamos dessa forma as interações e tomada de decisão em grupo, que são essenciais para o desenvolvimento social do aluno. O professor, aplicador das atividades, observará as estratégias utilizadas por cada grupo para a resolução das atividades, assim como as dificuldades apresentadas por eles, fazendo intervenções, sempre que julgar necessário, sem, no entanto, dar as respostas prontas.

Para realização das tarefas, faz-se necessário que se dê tempo suficiente para os grupos. O tempo estimado por nós, a princípio, foi de cerca de 45 minutos para realização de cada atividade, sendo aceitas variações desse tempo dependendo do grau de dificuldade de cada atividade, o que será observado e relatado pelo professor/aplicador.

O professor/aplicador poderá realizar perguntas pertinentes à resolução ou ao conteúdo relacionado, sempre que achar que elas ajudarão na compreensão dos conteúdos matemáticos ou do algoritmo de resolução de cada item.

Após a resolução de cada atividade, os alunos poderão ser convidados a expor sua resolução e discuti-las com seus colegas e com o professor/aplicador. Esse momento de interação é importante para estimular uma maior participação dos alunos, embora a mediação do aplicador se faça necessária. Nesse momento os alunos terão a oportunidade de ter contato com as estratégias de resolução dos outros colegas, o que pode contribuir com um aumento do leque de resoluções de cada aluno.

O professor/aplicador deverá considerar todas as soluções construídas pelos alunos, mesmo aquelas que contenham erros ou inconsistências.

5.1 Atividade 1: Criptografando com Função Afim

Objetivo Geral: Mostrar como a função afim pode ser usada para criptografar mensagens de forma simples.

Objetivos Específicos:

- Calcular o valor numérico de uma função afim (cálculo de imagem);

- Calcular a função inversa de uma função afim, bem como a imagem inversa;
- Determinar as condições para bijeção de uma função afim.

Pré-requisitos:

- Definição de função e função afim;
- Definição de função injetora, sobrejetora e bijetora;
- Cálculo de valor numérico de funções (imagens);
- Cálculo de função inversa da função afim.

Recursos Didáticos: Papel, lápis, borracha, calculadora, quadro branco, marcador para quadro branco, computador, projetor multimídia e caderno de atividades.

Inicialmente, iremos relacionar números ao nosso alfabeto (o símbolo # representa um espaço em branco), com o auxílio da tabela abaixo:

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabela 11: Tabela de Associação Alfabeto-Numérica 1
Fonte: Do Autor

Portanto, cifrar uma mensagem recai no problema de permutar números por meio de uma regra *f*. Dessa forma, suponhamos que um casal apaixonado deseja trocar mensagens secretas, utilizando a tabela dada. Vamos ajudá-los a realizar tal intento, o primeiro passo a se tomar é definir a função cifradora, digamos $f(x) = 3x - 5$. Assim, por exemplo, à mensagem "AMO VOCÊ" associamos a sequência numérica 1 – 13 – 15 – 0 – 22 – 15 – 3 – 5, mas transmitimos a sequência: (-2) – 34 – 40 – (-5) – 61 – 40 – 4 – 10. Observe que não são usados sinais de pontuação e/ou acentuação gráfica.

a) Paulo deseja enviar a mensagem "VAMOS NOS ENCONTRAR". Qual seria a sequência numérica criptografada para essa mensagem?

b) Ao receber a mensagem, qual deve ser o passo a passo de Ana para ler (decodificar) a mensagem? Qual o conceito matemático associado ao processo de decodificar uma mensagem nos moldes dado?

c) Paulo recebe a sequência numérica: 55 – 10 – (-5) –10 – 37 – 4 – 40 – 37 – 55 – 49 – 40 – (-5) – (-2) – 43 – 40 – 52 – (-5) – (-2) – (-5) – (-2) – 58 – 31 – (-2). Decodifique a mensagem recebida por Paulo?

d) Um “espião” apoderou-se de um pedaço de papel no qual havia uma correspondência entre dois pares de números da sequência numérica decodificada por Paulo (item anterior) e ele sabe que a função codificadora é afim, seria ele capaz de ler qualquer outra mensagem trocada pelo casal? Em caso afirmativo, explique como isso seria feito?
e) Crie uma mensagem curta, codifique-a usando uma Função Afim de sua preferência e, envie-a para um grupo de sua escolha, indicando em sua mensagem qual foi a sua função escolhida. Certifique-se de que nenhum grupo receba mais de uma mensagem.
f) Decodifique a mensagem recebida pelo seu grupo.

Resultados Esperados:
a) Espera-se que o aluno seja capaz de fazer a correlação numérica entre letra e número de acordo com a tabela dada e, em seguida, consiga calcular adequadamente as imagens correspondentes, encontrando a sequência numérica criptografada;
b) Espera-se que o aluno seja capaz de identificar os passos necessários para se realizar a decodificação da mensagem, ou seja, que ele seja capaz de identificar e calcular as imagens inversas da sequência numérica encontrada no item anterior;
c) Espera-se que o aluno padronize o processo descrito e calculado no item anterior e decodifique a sequência numérica dada, encontrando a mensagem clara (original);
d) Espera-se que o aluno seja capaz de identificar a relação entre pares ordenados e os coeficientes da função já que, no caso da função afim, são suficientes dois pares para se determinar seus coeficientes. Espera-se também que o aluno seja capaz de descrever o passo a passo da montagem e resolução do sistema linear para a obtenção dos coeficientes da função afim.
e) A intenção é que o aluno seja capaz de entender o processo e de criar suas próprias mensagens criptografadas por este processo;
f) Espera-se que o aluno consiga desincriptar qualquer mensagem codificada por este método.

5.2 Atividade 2: Criptografando com Funções Quadráticas

Objetivo Geral: Mostrar como a função quadrática pode ser usada para criptografar mensagens desde que se restrinja seu domínio.

Objetivos Específicos:

- Calcular o valor numérico de uma função quadrática (cálculo de imagem);
- Calcular a função inversa de uma função quadrática, bem como a imagem inversa (quando existir);
- Determinar as condições para bijeção de uma função quadrática.

Pré-requisitos:

- Definição de função e função quadrática;
- Definição de função injetora, sobrejetora e bijetora;
- Cálculo de valor numérico de funções;
- Cálculo de função inversa da função quadrática.

Recursos Didáticos: Papel, lápis, borracha, calculadora, quadro branco, marcador para quadro branco, projetor multimídia e caderno de atividades.

Com base na tabela dada na atividade 5.1 e usando a função cifradora $f(x) = x^2 - 4x + 4$, faça o que se pede:

a) Cifre a mensagem "AMO A MATEMÁTICA";

b) Você recebeu a mensagem codificada: 9 – 289 – 324 – 361 – 4 – 9 – 1 – 169 – 121 – 1 – 16 – 49 – 144 – 1 – 169. Decodifique a mensagem (observe que serão necessárias algumas tentativas para as imagens inversas repetidas);

c) Quais os conceitos matemáticos envolvidos na resolução do item "b"?

d) A função cifradora $f(x) = x^2 - 4x + 4$ usada foi uma boa escolha? Por quê?

e) Como você faria para corrigir o problema das imagens inversas repetidas?

f) Crie uma mensagem curta, em seguida, usando uma Função Quadrática de sua escolha codifique-a e a envie para um grupo de sua preferência, não se esqueça de informar a função cifradora escolhida para que o outro grupo seja capaz de decifrar a mensagem.

g) Decodifique a mensagem recebida pelo seu grupo.

Resultados Esperados:

a) Espera-se que o aluno seja capaz de fazer a correlação numérica entre as letras da mensagem clara e os números dados na Tabela 11: Tabela de Associação Alfabeto-Numérica 1 (atividade 5.1) e, em seguida, consiga calcular adequadamente as imagens correspondentes,

encontrando a sequência numérica criptografada. O aluno mais atento poderá perceber a presença de "imagens repetidas";

b) Espera-se que o aluno seja capaz de identificar os passos necessários para se realizar a decodificação da mensagem, ou seja, que ele seja capaz de identificar e calcular as imagens inversas da sequência numérica encontrada no item anterior e, para as "imagens inversas repetidas", fazer a escolha correta, testando as opções;

c) Espera-se que o aluno seja capaz de identificar os conceitos de função inversa para função quadrática e de imagem inversa;

d) Espera-se que o aluno seja capaz de identificar a restrição existente para a existência de função inversa da função quadrática, ou seja, que o aluno seja capaz de usar, mesmo que de forma intuitiva, a ideia de bijeção como condição suficiente para a escolha da função cifradora. A intenção é que o aluno seja capaz de entender que para tornar uma função quadrática bijetora, basta restringir seu domínio, ou seja, tomar como domínio um subconjunto do conjunto $[x_V, +\infty)$ (ou $[-\infty, x_V)$) e, para o contra-domínio, o correspondente subconjunto de $[y_V, +\infty)$ (ou $[-\infty, y_V)$); fato este que pode ser melhor visualizado com o uso de um gráfico. No nosso caso, como fixamos o domínio, esperamos que o aluno perceba e comente este fato.

e) Espera-se que os alunos observem que como o domínio são números inteiros, escolhendo-se coeficientes também inteiros para nossa função cifradora, obteremos imagens inteiras (pela propriedade de fechamento para a adição e multiplicação de inteiros). Outra forma de evitar o problema de imagens repetidas seria tomar os valores do domínio maiores do que a coordenada de *x* do vértice;

f) A intenção é que o aluno seja capaz de entender o processo e, de criar suas próprias mensagens criptografadas por este processo;

g) Espera-se que o aluno consiga desincriptar qualquer mensagem codificada por este método.

5.3 Atividade 3: Criptografando com Função Exponencial e Logarítmica

Objetivo Geral: Mostrar como a função exponencial e a função logarítmica podem ser usadas para criptografar mensagens.

Objetivos Específicos:

- Calcular o valor numérico de uma função exponencial ou logarítmica (cálculo de imagem);
- Calcular a função inversa de uma função exponencial ou logarítmica, bem como a imagem inversa;
- Determinar as condições para bijeção de uma função exponencial ou logarítmica.

Pré-requisitos:

- Definição de função e função exponencial e logarítmica;
- Definição de função injetora, sobrejetora e bijetora;
- Cálculo de valor numérico de funções;
- Cálculo de função inversa da função exponencial e logarítmica.

Recursos Didáticos: Papel, lápis, borracha, calculadora, quadro branco, marcador para quadro branco, projetor multimídia e caderno de atividades.

Ainda com base na tabela dada na atividade 5.1, mas agora utilizando a função cifradora $f(x) = 2^x$, faça o que se pede:

a) Codifique a mensagem "CRIPTOGRAFAR É DIVERTIDO", usando a função dada no enunciado;

b) Você recebeu a mensagem codificada: 2 – 8192 – 32 – 2 – 8192 – 2 – 1048576 – 32 – 8192 – 2 – 1048576 – 512 – 8 – 2, que foi obtida ao se utilizar a função cifradora dada no enunciado. Decodifique-a;

c) Quais os conceitos matemáticos envolvidos nos dois itens anteriores?

d) Crie uma mensagem curta, codifique-a usando a função logarítmica $y = \log_{10} x$ e a envie para um grupo de sua preferência. Trabalhe com 4 casas decimais (após a vírgula);

e) Decodifique a mensagem recebida pelo seu grupo. Arredonde os valores para o inteiro mais próximo.

Resultados Esperados:

a) Espera-se que o aluno seja capaz de fazer a correlação numérica entre as letras da mensagem clara e os números dados na Tabela 11: Tabela de Associação Alfabeto-Numérica 1 (atividade 5.1) e, em seguida, consiga calcular adequadamente as imagens correspondentes, encontrando a sequência numérica criptografada;

b) Espera-se que o aluno seja capaz de identificar os passos necessários para se realizar a decodificação da mensagem, ou seja, que ele seja capaz de identificar e calcular as imagens inversas da sequência numérica dada no item enunciado. Busca-se também que o aluno seja capaz de sistematizar a obtenção de imagens inversas para a função dada, com o auxílio da calculadora científica;

c) Espera-se que o aluno seja capaz de identificar a relação de função inversa que existe entre função exponencial e função logarítmica;

d) Espera-se que o aluno compreenda que tanto a função exponencial como a logarítmica podem ser utilizadas para cifrar uma mensagem. A intenção é que o aluno seja capaz de entender o processo e, de criar suas próprias mensagens criptografadas também utilizando a função logarítmica;

e) Espera-se que o aluno consiga desincriptar qualquer mensagem codificada por uma função logarítmica, encontrando sua respectiva função inversa e, calculando as imagens inversas necessárias para tal desígnio.

5.4 Atividade 4: Criptografando com Matrizes

Objetivo Geral: Mostrar como Matrizes podem ser usadas para criptografar mensagens.

Objetivos Específicos:

- Definir Matrizes e estabelecer seus principais tipos;
- Trabalhar com a multiplicação de matrizes;
- Determinar as condições para inversão de matrizes, bem como calcular as matrizes inversas.
- Calcular o determinante de matrizes

Pré-requisitos:

- Operações com Matrizes, em especial a multiplicação;
- Saber determinar a inversa de uma matriz;
- Cálculo do determinante de uma matriz.

Recursos Didáticos: Papel, lápis, borracha, calculadora, quadro branco, marcador para quadro branco, projetor multimídia e caderno de atividades.

Após terem suas mensagens decodificadas por um espião, suponhamos agora que Ana e Paulo combinem de utilizar as matrizes $A=\begin{pmatrix}1 & 2\\ 2 & 3\end{pmatrix}$ e $A^{-1}=\begin{pmatrix}-3 & 2\\ 2 & -1\end{pmatrix}$ como chaves para codificar suas mensagens. Para transmitir a mensagem "TESTE DE CHAVE", Paulo inicialmente monta uma matriz mensagem M (usando a tabela dada na atividade 5.1) dispondo a sequência numérica associada à mensagem em colunas e completando a posição restante com o 0, obtendo:

$$M=\begin{pmatrix}20 & 19 & 5 & 4 & 3 & 1 & 5\\ 5 & 20 & 0 & 5 & 8 & 22 & 0\end{pmatrix}.$$

Feito isto, codificou a mensagem usando a matriz A, calculando:

$$AM=\begin{pmatrix}1 & 2\\ 2 & 3\end{pmatrix}\begin{pmatrix}20 & 19 & 5 & 4 & 3 & 1 & 5\\ 5 & 20 & 0 & 5 & 8 & 22 & 0\end{pmatrix}$$
$$=\begin{pmatrix}30 & 59 & 5 & 14 & 19 & 45 & 5\\ 55 & 98 & 10 & 23 & 30 & 68 & 10\end{pmatrix},$$

e transmite a sequência numérica: 30 – 55 – 59 – 98 – 5 – 10 – 14 – 23 – 19 – 30 – 45 – 68 – 5 – 10. Para decodificar (ler) a mensagem recebida, Ana, deve restaurar o formato da matriz AM, em seguida, com a chave decodificadora A^{-1} recupera a matriz M através da identidade matricial:

$$M=A^{-1}.(A.M)$$
$$M=\begin{pmatrix}-3 & 2\\ 2 & -1\end{pmatrix}.\begin{pmatrix}30 & 59 & 5 & 14 & 19 & 45 & 5\\ 55 & 98 & 10 & 23 & 30 & 68 & 10\end{pmatrix}$$
$$=\begin{pmatrix}20 & 19 & 5 & 4 & 3 & 1 & 5\\ 5 & 20 & 0 & 5 & 8 & 22 & 0\end{pmatrix}.$$

Observe que não são usados sinais de pontuação e/ou acentuação gráfica.

a) Ana quer enviar a mensagem "TE CURTO DE MONTÃO", qual deve ser a sequência numérica transmitida para Paulo?

b) Recebida a mensagem acima por Paulo, qual será o procedimento dele para poder ler (decodificar) a mensagem? Qual o conceito matemático, associado ao processo de decodificar a mensagem, feito por Paulo?

c) Ana recebe a mensagem codificada: 33 – 52 – 33 – 51 – 54 – 88 – 48 – 81 – 33 – 51 – 26 – 46 – 45 – 72 – 15 – 29 – 34 – 53. Qual a mensagem original (após ser decodificada) enviada por Paulo?

d) Caso um "espião" venha a se apoderar da mensagem do item anterior e, sendo conhecida a tabela da atividade 5.1, essas informações seriam suficientes para decodificá-la? Em caso Negativo, o que mais o espião precisa para poder decodificar a mensagem interceptada?

e) Crie uma mensagem curta, usando uma matriz cifradora 2x2 (matriz A) de sua escolha; envie-a para outro grupo, não se esqueça de informar ao grupo escolhido a matriz A^{-1} que servirá para a decodificação de sua mensagem.

f) Decodifique a mensagem recebida pelo seu grupo.

Resultados Esperados:

a) Espera-se que o aluno seja capaz de fazer a correlação entre as letras da mensagem clara e os números dados na tabela e, realizar a multiplicação das matrizes mensagem M e matriz chave A, encontrando a matriz codificada AM;

b) Espera-se que o aluno seja capaz de identificar os passos necessários para se realizar a decodificação da mensagem, ou seja, que ele seja capaz de identificar e calcular a matriz inversa A^{-1} da matriz A;

c) Espera-se que o aluno padronize o processo descrito e calculado no item anterior e decodifique a sequência numérica dada, encontrando a mensagem clara (original);

d) Espera-se que o aluno seja capaz de identificar a importância da matriz A^{-1} para a decodificação de uma mensagem (usando matrizes);

e) A intenção é que o aluno seja capaz de entender o processo e, de criar suas próprias mensagens criptografadas por este processo, inclusive, efetuando o cálculo da matriz inversa A^{-1} de sua matriz A, escolhida para a codificação de sua mensagem;

f) Espera-se que o aluno consiga desincriptar qualquer mensagem codificada por este método.

5.5 Atividade 5: Criptografando Pelas Cifras de Hill

Objetivo Geral: Mostrar como Matrizes associadas a conceitos básicos de congruência podem ser usadas para criptografar mensagens.

Objetivos Específicos:

- Definir Matrizes e estabelecer seus principais tipos;
- Definir congruência e algumas de suas principais propriedades;
- Trabalhar com a multiplicação de matrizes;
- Determinar as condições para inversão de matrizes, bem como calcular as matrizes inversas;
- Calcular o determinante de matrizes;
- Trabalhar com módulo de um número inteiro.

Pré-requisitos:

- Operações com Matrizes, em especial a multiplicação;
- Saber trabalhar as principais operações com módulo de um número inteiro positivo;
- Saber determinar a inversa de uma matriz;
- Cálculo do determinante de uma matriz.

Recursos Didáticos: Papel, lápis, borracha, calculadora, quadro branco, marcador para quadro branco, projetor multimídia e caderno de atividades.

A abordagem metodológica, bem como as ideias expostas a seguir foram baseadas em (ANTON e RORRES, 2001) e (HEFEZ, 2011), os exemplos são de autoria nossa.

Primeiramente vamos associar cada letra do texto comum (claro) e do texto cifrado, excetuando-se o "Z", a um valor numérico que especifica sua posição no nosso alfabeto, dado pela tabela de associação abaixo

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**
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	0

Tabela 12: Tabela de Associação Alfabeto-Numérica 2
Fonte: Do Autor

Por motivos que ficarão claros mais tarde, damos a "Z" o valor de 0.

Nos casos mais simples de cifras de Hill (nosso caso), transformamos pares sucessivos de texto comum em texto cifrado pelo seguinte procedimento:

1º Passo: Escolha uma matriz 2x2 $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ com entradas inteiras para efetuar a codificação. Condições adicionais sobre ***A*** serão impostas mais tarde.

2º Passo: Agrupe letras sucessivas do texto comum em pares, adicionando uma letra fictícia (no nosso caso repetiremos a última letra do texto claro) para completar o último par se o texto comum tiver um número ímpar de letras. Substitua cada letra do texto comum por seu equivalente numérico.

3º Passo: Converta cada par sucessivo $p_1 p_2$ de letras do texto comum em um vetor coluna (matriz 2x1) $p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ e forme o produto $\boldsymbol{Ap}$. Chamamos $\boldsymbol{p}$ de *vetor comum* e $\boldsymbol{Ap}$ o correspondente *vetor cifrado.*

4º Passo: Converta cada vetor cifrado em seu equivalente alfabético, usando a congruência (mod 26) e a tabela dada anteriormente.

Exemplo 1: Usando a matriz codificadora $A = \begin{pmatrix} 7 & 5 \\ 5 & 8 \end{pmatrix}$, desejamos codificar a mensagem: "CRIPTOGRAFIA" através da cifra de Hill.

Solução:

Vamos agrupar as letras do texto comum em pares, obtendo: CR – IP – TO – GR – AF – IA. Usando a tabela dada, encontramos a correspondência numérica: (3; 18) – (9; 16) – (20; 15) – (7; 18) – (1; 6) – (9; 1). Para codificar o par "CR", devemos efetuar o produto matricial $Ap = \begin{pmatrix} 7 & 5 \\ 5 & 8 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 18 \end{pmatrix} = \begin{pmatrix} 111 \\ 159 \end{pmatrix}$. Observe que os números 111 e 159 não possuem equivalente alfabético na tabela dada (Tabela 12: Tabela de Associação Alfabeto-Numérica 2). Para resolver esse problema nós fazemos o seguinte acordo: *"Sempre que aparecer um inteiro maior que 25, ele será substituído pelo resto da divisão desse inteiro por 26"*. Como o resto da divisão por *26* é sempre um dos números *0, 1, 2, ..., 25*, este procedimento sempre fornece um inteiro com equivalente alfabético dado pela nossa tabela. Por esse motivo, demos o valor 0 ao "Z".

Assim, o vetor $\begin{pmatrix} 111 \\ 159 \end{pmatrix}$ deve ser substituído por $\begin{pmatrix} 7 \\ 3 \end{pmatrix}$, pois 7 é o resto da divisão de 111 por 26 e 3 é o resto da divisão de 159 por 26, e obtemos o par de letras cifradas "GC".

As contas para os outros vetores cifrados são:

$$\begin{pmatrix}7 & 5\\ 5 & 8\end{pmatrix}.\begin{pmatrix}9\\16\end{pmatrix}=\begin{pmatrix}143\\173\end{pmatrix} ou \begin{pmatrix}13\\17\end{pmatrix}$$
$$\begin{pmatrix}7 & 5\\ 5 & 8\end{pmatrix}.\begin{pmatrix}20\\15\end{pmatrix}=\begin{pmatrix}215\\220\end{pmatrix} ou \begin{pmatrix}7\\12\end{pmatrix}$$
$$\begin{pmatrix}7 & 5\\ 5 & 8\end{pmatrix}.\begin{pmatrix}7\\18\end{pmatrix}=\begin{pmatrix}139\\179\end{pmatrix} ou \begin{pmatrix}9\\23\end{pmatrix}$$
$$\begin{pmatrix}7 & 5\\ 5 & 8\end{pmatrix}.\begin{pmatrix}1\\6\end{pmatrix}=\begin{pmatrix}37\\53\end{pmatrix} ou \begin{pmatrix}11\\1\end{pmatrix}$$
$$\begin{pmatrix}7 & 5\\ 5 & 8\end{pmatrix}.\begin{pmatrix}9\\1\end{pmatrix}=\begin{pmatrix}68\\53\end{pmatrix} ou \begin{pmatrix}16\\1\end{pmatrix}$$

Esses vetores correspondem, respectivamente, aos pares de textos cifrados “MQ”, “GL”, “IW”, “KA”, “PA”. Juntando todos os pares de texto cifrados, obtemos a mensagem cifrada completa: GC – MQ – GL – IW – KA – PA, que seria transmitida como uma única cadeia de letras sem espaços: “GCMQGLIWKAPA”.

Como o texto comum foi agrupado em pares e criptografado por uma matriz 2x2, dizemos que a cifra de Hill do nosso exemplo é uma *2-cifra de Hill*. Evidentemente também é possível agrupar o texto comum em ternos e criptografar com uma matriz 3x3 com entradas inteiras, esta cifra é chamada *3-cifra de Hill*. Em geral, para uma *n-cifra de Hill* agrupamos o texto comum em conjuntos de *n* letras e criptografamos usando uma matriz *n* x *n* de entradas inteiras.

Aritmética Modular: No nosso exemplo substituímos os inteiros maiores do que 25 pelos seus respectivos restos pela divisão por 26. Esta técnica de trabalhar com os restos é a base de uma parte da Matemática chamada Aritmética Modular. Tendo em vista sua importância em criptografia, iremos fazer uma breve pausa para elaborar algumas das principais ideias desta área.

Congruência: Em Aritmética Modular nós supomos dado um inteiro positivo *m*, chamado módulo e consideramos “iguais” ou “equivalentes” (congruentes) em relação a esse módulo quaisquer dois inteiros cuja diferença é um múltiplo inteiro desse módulo. Mais precisamente, temos a seguinte definição.

Definição 1: Dados um número inteiro positivo *m* e dois inteiros *a* e *b* quaisquer, dizemos que *a* é congruente a *b* módulo *m*, e escrevemos $a \equiv b \pmod{m}$, se *a* – *b* é um múltiplo inteiro de *m*.

Por exemplo, $7 \equiv 2 \pmod 5$, já que os restos da divisão de 7 e de 2 por 5 são iguais a 2. Da mesma forma, $19 \equiv 3 \pmod 2$, pois os restos da divisão de 19 e de 3 por 2 são iguais a 1. Outros exemplos de congruência: $-1 \equiv 25 \pmod{26}$, $12 \equiv 0 \pmod 4$.

Classes Residuais: Dado um número inteiro *m > 1*, vamos repartir o conjunto *Z* dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por *m*. Isto nos dá a seguinte partição de *Z*:

$$[0] = \{x \in Z;\ x \equiv 0 \pmod m\},$$
$$[1] = \{x \in Z;\ x \equiv 1 \pmod m\},$$
$$\ldots$$
$$[m-1] = \{x \in Z;\ x \equiv m-1 \pmod m\}$$

Paramos em $[m-1]$, pois se tem que $[m] = [0], [m+1] = [1], \ldots$

O conjunto

$$[a] = \{x \in Z;\ x \equiv a \pmod m\}$$

é chamado de *classe residual módulo m* do elemento *a* de *Z*. O conjunto de todas as classes residuais módulo *m* será representado por Z_m. Portanto,

$$Z_m = \{[0], [1], \ldots, [m-1]\}.$$

Por exemplo, se *m = 2*, então

$$[0] = \{x \in Z;\ x \equiv 0 \pmod 2\} = \{x \in Z;\ x \text{ é } par\} \text{ e}$$
$$[1] = \{x \in Z;\ x \equiv 1 \pmod 2\} = \{x \in Z;\ x \text{ é } ímpar\}.$$

Temos também que $[a] = [0]$ se, e somente se, *a* é par e $[a] = [1]$ se, e somente se, *a* é ímpar.

Recíproco ou Inverso Multiplicativo: Na Aritmética usual, cada número não nulo *a* tem um *recíproco*, ou *inverso multiplicativo*, denotado por a^{-1}, tal que

$$a.a^{-1} = 1.$$

Na Aritmética Modular nós temos o seguinte conceito correspondente:

Definição 2: Dado um número *a* em Z_m, dizemos que um número a^{-1} em Z_m é um recíproco, ou inverso multiplicativo de *a* módulo *m* se

$$a.a^{-1} \equiv a^{-1}.a \equiv 1 \pmod m.$$

Pode ser provado que se *a* e *m* não têm fatores primos em comum, então *a* tem um único recíproco módulo *m*. Reciprocamente, se *a* e *m* têm um fator primo em comum, então *a* não tem recíproco módulo *m*.

Exemplos 2: O número 3 tem um recíproco módulo 26, pois 3 e 26 não têm fatores primos em comum. Este recíproco pode ser obtido, encontrando o número *x* em Z_{26} que satisfaz a congruência $3x \equiv 1 \pmod{26}$. Embora existam métodos gerais para resolver tais congruências, isto não será abordado aqui, pois nos levaria para muito longe do nosso objetivo. Contudo, como 26 é relativamente pequeno, esta congruência pode ser resolvida por inspeção, testando uma por uma cada solução possível de 0 a 25. Fazendo isto, encontramos que *x = 9* é a solução procurada, pois $3.9 = 27 \equiv 1 \pmod{26}$.

Exemplos 3: O número 4 não possui recíproco mod 26, pois 4 e 26 têm o número 2 como fator primo comum.

Para consultas futuras, fornecemos a seguinte tabela de recíprocos mod 26:

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Tabela 13: Tabela de Recíprocos mod 26
Fonte: (ANTON e RORRES, 2001)

Decifrando a Cifra de Hill: Cada cifra útil deve possuir um procedimento para decifrar. Para decifrar as cifras de Hill, usamos a inversa (*mod 26*) da matriz codificadora. Para ser preciso, se *m* é um inteiro positivo, dizemos que uma matriz *A* com entradas em Z_m é invertível módulo *m* se existir uma matriz *B* com entradas em Z_m tal que

$$A.B = B.A = I \pmod{m}.$$

Suponha agora que $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ é invertível módulo 26 e que esta matriz é usada para uma 2-cifra de Hill. Se $p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ é um vetor comum, então $\boldsymbol{c = A.p}$ é o correspondente vetor cifrado. Para recuperar o vetor $\boldsymbol{p}$ devemos multiplicar ambos os lados da igualdade anterior por $\boldsymbol{A^{-1}}$ e obter $\boldsymbol{p = A^{-1}.c}$. Assim, cada vetor comum pode ser recuperado do correspondente vetor cifrado pela multiplicação, à esquerda, por $\boldsymbol{A^{-1}}$ **(*mod 26*)**.

Em Criptografia é importante saber quais matrizes são invertíveis módulo 26 e como obter suas inversas. Em Aritmética comum, uma matriz quadrada *A* é invertível se, e somente se, $\det(A) \neq 0$ ou, equivalentemente, *det (A)* tem um recíproco. O teorema seguinte é o análogo deste resultado em Aritmética Modular.

Teorema 1: Uma matriz quadrada *A* com entradas em Z_m é invertível módulo *m* se, e somente se, o resíduo de *det (A)* módulo *m* tem um recíproco módulo *m*.

Como o resíduo de *det (A)* módulo *m* terá um recíproco módulo *m* se, e somente se, este resíduo e *m* não tiverem fator primo em comum, temos o seguinte corolário.

Corolário 1: Uma matriz quadrada *A* com entradas em Z_m é invertível módulo *m* se, e somente se, *m* e o resíduo de *det (A)* módulo *m* não têm fatores primos comuns.

Como os únicos fatores primos de m = 26 são 2 e 13, temos o seguinte corolário que é útil em criptografia.

Corolário 2: Uma matriz quadrada *A* com entradas em Z_{26} é invertível módulo *26* se, e somente se, o resíduo de *det (A)* módulo *26* não é divisível por 2 ou por 13.

Pode-se demonstrar (porém isto foge ao nosso objetivo) que se $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tem entradas em Z_{26} e se o resíduo de *det (A) = ad – bc (mod 26)* não é divisível por 2 ou por 13, então a inversa de *A (mod 26)* é dada por

$$A^{-1}=(ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}(\text{mod } 26).$$

Onde $(ad-bc)^{-1}$ é o recíproco do resíduo de $ad-bc\,(\text{mod } 26)$.

Exemplo 4: Encontre a inversa da matriz $A=\begin{bmatrix} 7 & 5 \\ 5 & 8 \end{bmatrix}(\text{mod } 26)$.

Solução:

$$\det(A)=7.8-5.5=31\equiv 5\,(\text{mod } 26).$$

Usando a tabela (Tabela 13: Tabela de Recíprocos mod 26), encontramos o seu recíproco que é

$$(ad-bc)^{-1}=5.x\equiv 1\,(\text{mod } 26)\Rightarrow x\equiv 21\,(\text{mod } 26)\Rightarrow x=21.$$

Assim, pela fórmula dada, tem-se

$$A^{-1}=(ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}(\text{mod } 26)=21.\begin{bmatrix} 8 & -5 \\ -5 & 7 \end{bmatrix}(\text{mod } 26)=\begin{bmatrix} 168 & -105 \\ -105 & 147 \end{bmatrix}(\text{mod } 26)\equiv$$

$$\equiv\begin{bmatrix} 12 & 25 \\ 25 & 17 \end{bmatrix}(\text{mod } 26).$$

Verificando,

$$A.A^{-1}=\begin{bmatrix} 7 & 5 \\ 5 & 8 \end{bmatrix}\begin{bmatrix} 12 & 25 \\ 25 & 17 \end{bmatrix}=\begin{bmatrix} 84+125 & 175+85 \\ 60+200 & 125+136 \end{bmatrix}=\begin{bmatrix} 209 & 260 \\ 260 & 261 \end{bmatrix}\equiv\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}(\text{mod } 26).$$

Analogamente, $A^{-1}.A = I \pmod{26}$.

Exemplo 5: Decifre a *2-cifra de Hill* criptografada no exemplo 1.

Solução:

A mensagem cifrada é "GCMQGLIWKAPA", cujo equivalente numérico é (7; 3), (13; 17), (7; 12), (9; 23), (11; 1), (16; 1). Para obter os pares de texto comum nós devemos multiplicar cada vetor cifrado pela inversa de *A (mod 26)*, à esquerda, ou seja,

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}7\\3\end{bmatrix} = \begin{bmatrix}159\\226\end{bmatrix} \equiv \begin{bmatrix}3\\18\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}13\\17\end{bmatrix} = \begin{bmatrix}581\\614\end{bmatrix} \equiv \begin{bmatrix}9\\16\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}7\\12\end{bmatrix} = \begin{bmatrix}384\\379\end{bmatrix} \equiv \begin{bmatrix}20\\15\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}9\\23\end{bmatrix} = \begin{bmatrix}683\\616\end{bmatrix} \equiv \begin{bmatrix}7\\18\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}11\\1\end{bmatrix} = \begin{bmatrix}157\\292\end{bmatrix} \equiv \begin{bmatrix}1\\6\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}16\\1\end{bmatrix} = \begin{bmatrix}217\\417\end{bmatrix} \equiv \begin{bmatrix}9\\1\end{bmatrix} \pmod{26}.$$

Pela tabela (Tabela 12: Tabela de Associação Alfabeto-Numérica 2), os equivalentes alfabéticos destes vetores são: CR – IP – TO – GR – AF – IA, que nos fornecem a mensagem: "CRIPTOGRAFIA".

Agora é com você: Imagine que você é o comandante de uma tropa que está posicionada no campo de batalha e aguarda seus comandos, usando a *2-cifra de Hill* e a matriz codificadora $A = \begin{pmatrix}7 & 5\\1 & 8\end{pmatrix}$, você deseja codificar a frase: "ATACAR AO AMANHECER" e enviá-la para suas tropas de maneira segura. Observe que após agrupar o texto comum em pares de letras e adicionar a letra fictícia no final, obtemos: AT – AC – AR – AO – AM – AN – HE – CE – RR. Usando a tabela de associação alfabeto-numérica, encontramos o equivalente numérico: (1; 20) – (1; 3) – (1; 18) – (1; 15) – (1; 13) – (1; 12) – (8; 5) – (3; 5) – (18; 18). Para codificar os pares do texto comum devemos efetuar o produto da matriz ***A*** por cada um dos vetores correspondentes aos pares de letras dados (vetor ***p***). Não se esqueça de que os elementos da matriz produto (vetor ***Ap***) obtida, que forem maiores ou iguais a 26, deverão ser substituídos pelos resíduos de sua congruência (mod 26), ou seja, devemos tomar o resto de sua divisão

por 26. Procedendo dessa forma, sempre teremos uma associação da mensagem original com letras da tabela dada (Tabela 12: Tabela de Associação Alfabeto-Numérica 2), isto é, sempre teremos uma mensagem que pode ser transformada em letras do nosso alfabeto.

a) Após codificar a frase dada no enunciado, quais os vetores ***Ap*** correspondentes à codificação? Como fica a frase codificada?

b) Suponha que você recebeu a frase codificada do item anterior, como você faria para decodificá-la? Você seria capaz de encontrar a matriz decodificadora $A^{-1} \pmod{26}$?

c) Quais os conceitos matemáticos envolvidos nos processos de codificação e decodificação da mensagem dada?

d) Crie uma mensagem curta e, usando a matriz ***A***, codifique-a e a envie para outro grupo de sua escolha;

e) Decodifique a mensagem que seu grupo recebeu, utilizando a matriz $A^{-1} \pmod{26}$.

Resultados Esperados:

a) Espera-se que o aluno seja capaz de fazer a correlação entre as letras da mensagem clara e os números dados na tabela e, realizar a multiplicação das matrizes mensagem ***p*** e matriz chave ***A***, encontrando as matrizes codificadas ***Ap***. Em seguida, espera-se que o aluno seja capaz de usar a ideia de congruência e realizar a associação dos números das matrizes ***Ap*** à uma nova mensagem (ininteligível) formada apenas por letras;

b) Espera-se que o aluno seja capaz de identificar os passos necessários para se realizar a decodificação da mensagem, ou seja, que ele seja capaz de identificar e calcular a matriz inversa $A^{-1} \pmod{26}$ da matriz ***A***;

c) Espera-se que o aluno seja capaz de identificar a presença do produto de matrizes, do cálculo do determinante de uma matriz, da congruência (mod 26) e do inverso multiplicativo (mod 26) para a codificação e decodificação de uma mensagem (nesses moldes);

d) A intenção é que o aluno seja capaz de entender o processo e criar suas próprias mensagens criptografadas por este processo, inclusive efetuando o cálculo da matriz inversa $A^{-1} \pmod{26}$ de sua matriz ***A***, escolhida para a codificação;

e) Espera-se que o aluno consiga desincriptar qualquer mensagem codificada por este método.

6 A ENGENHARIA DIDÁTICA E O NOSSO TRABALHO

Este capítulo é destinado a explicar como a Engenharia Didática foi aplicada em nosso trabalho, onde cada fase da Engenharia Didática foi trabalhada, ajudando em uma melhor compreensão de sua estrutura.

6.1 Fase das Análises Preliminares

Dentro do contexto (macroengenharia e microengenharia) apresentamos o tema Criptografia como motivador, objetivando desencadear situações-problema para uma melhor compreensão dos conteúdos de funções e matrizes, estudados no Ensino Médio; além de introduzir conhecimentos novos, como os conceitos de Aritmética Modular e inversa de funções quadráticas. Assim a Engenharia Didática relaciona os conceitos matemáticos e as situações didáticas propostas pelo educador.

Na fase das análises preliminares, foi realizada uma pesquisa bibliográfica, com o objetivo de investigar o tema Criptografia, sua história e aplicações. Foi realizado também um estudo exploratório do tema, buscando aliá-lo aos conteúdos matemáticos trabalhados no Ensino Médio, desenvolvendo atividades didáticas, buscando reforçar esses conteúdos por parte dos alunos, além de um conhecimento maior sobre o tema. Foi nesta fase, também, que ocorreu o primeiro contato com o campo de pesquisa e a população escolhida.

Novamente fazendo um paralelo com a nossa pesquisa, as variáveis macro-didáticas foram o tema Criptografia e os conteúdos do Ensino Médio, em especial funções e matrizes, e novos conteúdos (Aritmética Modular e inversa de função quadrática), pois possibilitam o desenvolvimento de atividades didáticas que levem os alunos a reforçarem esses conteúdos. As variáveis micro-didáticas são os conteúdos de matemática específicos envolvidos na resolução de cada uma das atividades. Buscou-se uma relação do conteúdo de matemática do Ensino Médio com as atividades propostas que levem o aluno a adquirir conceitos significativos sobre o tema. Dentro do contexto da concepção, das dificuldades e obstáculos encontrados pelos alunos, tentou-se delimitar e compreender as variáveis didáticas, as quais foram analisadas no decorrer do desenvolvimento das atividades didáticas.

6.2 Fase das Análises a Priori

No nosso trabalho, na fase das análises a priori, buscou-se prever as possíveis ações e comportamentos dos estudantes durante a resolução da atividade proposta, indicando de que forma as atividades propostas proporcionariam a aprendizagem desejada. Foi nesta fase que desenvolvemos toda a sequência didática aplicada na fase de experimentação, com base na fase de análises preliminares e no referencial teórico.

6.3 Fase da Experimentação

Durante a fase de Experimentação foi aplicada a sequência didática programada durante as fases anteriores. A sequência didática foi realizada em parceria com a Escola Estadual de Ensino Fundamental e Médio Antônio Batista Belo de Carvalho. A pesquisa foi desenvolvida na turma do 2º ano do turno vespertino, com apoio total da professora de Matemática Ana Silvia Bentes Furtado, titular da turma. Antes do início da aplicação da sequência didática houve uma reunião com a professora, na qual foram determinadas as quantidades de encontros e de aulas necessárias para desenvolvimento das atividades. Também foram feitas as previsões de recursos/materiais que seriam utilizados.

As atividades foram desenvolvidas ao longo de seis encontros, contando com duas aulas de 45 minutos cada encontro, distribuídos ao longo de duas semanas, durante os dias 24, 25, 26 de novembro e 01, 02 e 03 de dezembro de 2015. Em cada encontro foram realizadas tarefas distintas e imprescindíveis à realização de nossa atividade.

Os relatórios dos encontros foram feitos nos respectivos dias desses encontros, imediatamente após as aulas, quando ainda não se havia realizado a análise das soluções, análise esta que se encontra descrita no item 6.4 (Fase das Análises a Posteriori e Validação).

6.3.1 Primeiro Encontro

No 1º encontro, primeiramente, realizou-se a aplicação de um questionário pré-atividade (conforme APÊNDICE A) para auxiliar a análise a posteriore e validação. Em seguida, o trabalho foi apresentado aos alunos, com a realização de uma palestra sobre o tema Criptografia. Além disso, foi passado aos alunos o trailler do filme “O Jogo da Imitação” que

conta a história de Alan Turing e seus colaboradores em sua batalha para quebrar o código nazista gerado pela máquina Enigma. Também foram indicadas aos alunos as leituras de livros que têm o tema Criptografia como cerne.

6.3.2 Segundo Encontro

Durante o 2º encontro, antes de iniciar a aula de revisão, perguntou-se aos alunos alguns conceitos referentes à palestra da aula anterior, com intuito de reforçá-los, a resposta foi positiva por uma grande parte dos alunos, o que nos deixou satisfeitos e esperançosos em relação às etapas seguintes. Em seguida, procedeu-se a revisão do conteúdo de Funções, abordamos vários conceitos preliminares e associaciados, como por exemplo, Conjuntos Numéricos, Relações, Pares Ordenados, Função Sobrejetora, Injetora, Bijetora, Função Inversa e Função Afim. O professor orientador Hugo Diniz se fez presente neste encontro e fez registros fotográficos e pessoais, os quais pretendemos compartilhar na fase de Análise a Posteriori.

6.3.3 Terceiro Encontro

No 3º encontro, primeiramente, antes de começar a aula propriamente dita, foram feitas algumas perguntas referentes ao conteúdo trabalhado na aula anterior, sondando se os alunos ainda recordavam o que havia sido tratado, tivemos uma resposta satisfatória, algumas respostas desconexas, mas no geral boa participação e entusiasmo. Em seguida, procedeu-se a continuação da aula de revisão, na qual foram abordadas, inicialmente, formas de se reconhecer uma função e também reconhecer injetividade, sobrejetividade e bijetividade graficamente. Logo após, foi trabalhada a revisão dos temas: Funções Quadrática, Exponencial e Logarítmica. Abordamos as características de cada função e suas principais propriedades. A professora titular da turma esteve presente e fez registros de imagem e pessoais e também participou com comentários para ajudar a melhorar o entendimento do assunto.

6.3.4 Quarto Encontro

Durante o 4º encontro, primeiramente, por motivos de afinidade entre os alunos, a turma foi dividida em 5 grupos, sendo 3 grupos de 5 componentes, 1 grupo de 4 e 1 de 3 componentes. No transcorrer da Atividade 2 chegaram 3 alunos atrasados e estes, também por motivos de relacionamento, preferiram formar um novo grupo, ficando a turma dividida em 6 grupos. Veja as imagens dos grupos abaixo (Figura 17: Fotos dos Grupos). Após a entrega do material didático impresso (apostila encontrada no APÊNDICE C) contendo as atividades propostas, procedeu-se a leitura do enunciado da primeira atividade (Criptografando com Função Afim) em conjunto com os alunos para auxiliar na concentração e entendimento do que se pretendia em cada item dessa atividade. Após esse momento, os alunos se concentraram na execução dos itens, tendo sido disponibilizado, em média, 10 minutos para a resolução de cada item. Ainda nesse encontro, iniciou-se a segunda atividade (Criptografando com Função Quadrática), na qual o mesmo procedimento foi adotado, ou seja, após a leitura conjunta do enunciado, disponibilizou-se cerca de 10 minutos para as tentativas de resolução de cada item. Infelizmente, devido ao tempo desse encontro ter se esgotado, tivemos que parar no item “b”, ficando os demais itens para serem abordados no próximo encontro.

Figura 17: Fotos dos Grupos
Fonte: Do Autor

6.3.5 Quinto Encontro

O 5º encontro, excepcionalmente, contou com um incremento de mais duas aulas de 45 minutos, concedidas pelo professor de biologia (por motivo de ausência), contando, ao todo, com quatro aulas de 45 minutos. Começou-se com uma repetição do item “b” da atividade 2, pois ela não havia sido bem compreendida pelos alunos (problema com as “imagens inversas repetidas”). Após serem dirimidas as dúvidas a questão foi resolvida pela maioria dos alunos. O item “c” parece ter sido resolvido sem maiores problemas. O item “d” mesmo após uma discussão antecipada durante a resolução do item “b” não foi bem compreendido e novamente houve a necessidade de comentários adicionais para ajudar na compreensão (dificuldades em relacionar a escolha da função com a determinação da posição do vértice para evitar problema de “imagens repetidas”). O item “e” é uma consequência direta do item “d”, mesmo assim muitos alunos voltaram a relatar que não sabiam como resolver este item. Novamente se fez necessário a interferência com exemplos e comentários

para auxiliar o entendimento. No item “f”, a função cifradora poderia ser escolhida, mesmo assim houve alunos que não compreederam o que se pretendia, outra vez tivemos que explicar o que se pretendia com o comando do item, alguns tiveram dificuldades até mesmo para escolher uma função quadrática. O item “g” parece ter sido compreendido, mas teremos certeza apenas quando analisarmos as respostas (as respostas serão analisadas na fase de análise a posteriori e validação). Em seguida, passou-se para a atividade 3 (Criptografando com Função Exponencial e Logrítmica), após uma rápida apresentação da atividade e de um exemplo sobre o item “a”, os alunos parecem ter compreendido bem o que se pretendia neste item e a maioria parece tê-lo resolvido com êxito. O item “b” necessitou de uma explicação de como se obter a função inversa de uma função exponencial e de como se calcular imagens inversas, após isto, os alunos parecem ter conseguido resolver este item. O item “c” aparentemente foi bem compreendido e os alunos o resolveram sem muitas perguntas. Os itens “d” e “e” necessitaram de uma pequena explicação sobre o que se pretendia, mas os alunos parecem ter assimilado bem e a resolução parece ter transcorrido normalmente. Na sequência foi feita uma pausa de 15 minutos para descanso e lanche. As atividades recomeçaram, na sequência, com a resolução da atividade 4 (Criptografando com Matrizes), como o conteúdo havia sido trabalhado recentemente pela professora com os alunos, foi feita apenas uma leitura conjunta, uma explicação do mecanismo de criptografia e descriptografia, utilizando produto de matrizes, depois eles ficaram a vontade para resolver os itens. O item “a” parece ter sido bem compreendido e aparentemente todos os grupos o resolveram. Os itens “b” e “c” necessitaram apenas de um breve comentário sobre a importância da matriz inversa para a desincriptação de uma mensagem criptografada nos moldes do item “a”. Durante a resolução do item “c”, os alunos encontraram um erro na sequência numérica codificada fornecida no enunciado (mantivemos esse erro no Apêndice C). Este fato nos deixou bastante satisfeitos, pois percebemos que eles estavam muito motivados na resolução das atividades, tanto que conseguiram perceber um erro que nós havíamos deixado passar. Logicamente o erro foi corrigido e a mensagem foi decodificada, ao menos pela maioria dos aluns. O item “d” parece ter sido compreendido, foram poucas as perguntas sobre este item. Os itens “e” e “f” eram os itens em que a escolha da frase e da matriz codificadora era de livre escolha pelos alunos e nos quais havia interatividade entre os grupos. Eles parecem ter sido bem compreendidos, pois todas as atividades apresentam esses tipos de itens no final. No decorrer da atividade 4 foi percebido por nós e relatado pelos alunos um cansaço e um desgaste (em virtude da duração deste encontro), veremos no decorrer das análises das respostas como este fato pode ter interferido no desempenho deles.

6.3.6 Sexto Encontro

O 6º encontro começou com uma apresentação da cifra de Hill, e com a resolução de um exemplo bastante simples de uma 2-cifra de Hill. Em seguida, foram apresentados aos alunos alguns tópicos de Aritmética Modular (Congruências, Classes Residuais, Recíproco ou Inverso Multiplicativo) que são essenciais para o entendimento desse processo de cifragem. Logo depois, foi feita a leitura em conjunto da Atividade 5 (Criptografando com Cifras de Hill), uma vez que ficou claro o que se pretendia em cada item, foi dado aos alunos, em média, o tempo de 10 minutos para resolução de cada item. O item "a" foi resolvido sem grandes questionamentos, aparentemente a maioria dos alunos entendeu o que deveria ser feito. No item "b" houve questionamentos sobre a necessidade do cálculo da matriz $A^{-1}(\text{mod } 26)$ (inversa módulo 26 da matriz ***A***). Após ter sido esclarecido que se deveria tentar resolver, mesmo que não se conseguisse, todos tentaram. No que tange ao item "c", aparentemente, os alunos não apresentaram dificuldades de entendimento. Os itens "d" e "e" eram de interação entre os grupos, semelhantes aos outros feitos nas atividades anteriores, por isso não houve maiores dificuldades em seu entendimento.

Por fim, foi dado aos alunos o questionário pós-atividades para que pudessem registrar suas opiniões sobre a sequência didática realizada. Ficou combinado, como prêmio pelo empenho, que haveria um encontro não oficial no dia 7 de dezembro de 2015 para que os alunos pudessem assistir o filme "O Jogo da Imitação" na íntegra.

6.4 Fase da Análise a Posteriori e Validação

Os dados para realização da Análise a Posteriori e Validação foram coletados durante a fase de Experimentação, através das informações fornecidas pelos alunos nos questionários pré-atividades e pós-atividades, através de observações feitas pelo professor/pesquisador, pela professora/parceira e pelo professor/orientador, além de informações fornecidas pelos próprios alunos no transcorrer das atividades.

No transcorrer da apresentação do seminário sobre Criptografia, notou-se por parte dos alunos um nível de atenção e um "feedback" muito bom, o que nos deixou profundamente satisfeitos. Os alunos foram participativos e responderam a todas as perguntas feitas sobre a apresentação, mesmo que nem todas as respostas tenham sido coerentes.

Durante o 2º encontro iniciaram-se as aulas de revisão, nas quais foram abordados os temas mencionados na fase de Experimentação (Conjuntos Numéricos, Relações, Pares Ordenados, Função Sobrejetora, Injetora, Bijetora, Função Inversa e Função Afim). No decorrer da apresentação desses tópicos foram feitas perguntas aos alunos com o intuito de deteminar as carências, bem como os conhecimentos já trazidos por eles. Nesse momento, detectou-se uma grande carência de conceitos matemáticos básicos e fundamentais, o que tentamos imediatamente corrigir, mas devido ao pequeno tempo disponível esperamos tê-las sanado ao menos parcialmente. Já eram esperadas tais carências, no entanto, o que surpreendeu foi a profundidade delas. Contudo, como a atenção e a resposta (feedback) obtidos durante a aula foram muito boas, isso nos deixou esperançosos de que uma grande parte do que foi explicado tenha sido compreendido.

No 3º encontro com a continuidade das aulas de revisão, foram abordados temas como formas de se reconhecer uma função e também reconhecer injetividade, sobrejetividade e bijetividade graficamente, Funções Quadrática, Exponencial e Logarítmica. No transcorrer da apresentação de cada função, foram feitas perguntas para verificar a compreensão do conteúdo pelos alunos. Novamente tivemos uma resposta satisfatória, no geral. Verificou-se, outra vez, uma deficiência em conhecimentos básicos de matemática, buscamos sanar essas carências, sempre usando uma linguagem simples, trabalhando exemplos claros e com ênfase em reforços e repetição.

Em todas as atividades foi estimulado o uso da calculadora como elemento facilitador, de diferentes formas, segundo a necessidade de cada item. Eles ficaram livres para que ussasem a calculadora da forma que achassem mais conveniente. Logicamente, foram ensinadas as funções básicas que seriam úteis para a resoluções das atividades.

O grupo 6 não participou da atividade 1, por terem, seus componentes, chegado atrasados. Durante a atividade “Criptografando com Função Afim”, no item “a”, após atribuírem para cada letra da mensagem um valor numérico (com o auxílio da tabela de conversão alfabeto-numérica), os alunos procederam os cálculos das imagens da sequência numérica para obter uma nova sequência, codificando dessa forma a mensagem. Os grupos 1, 4 e 5 apresentaram soluções completas. Os grupos 2 e 3 apresentaram a sequência numérica cifrada, mas sem os cálculos necessários, acreditamos que os cálculos foram feitos mas não foram repassados para a folha de resoluções que foi entregue. Veja uma das soluções dos alunos (Figura 18: Resolução do Grupo1 para o item “a” da Atividade 1).

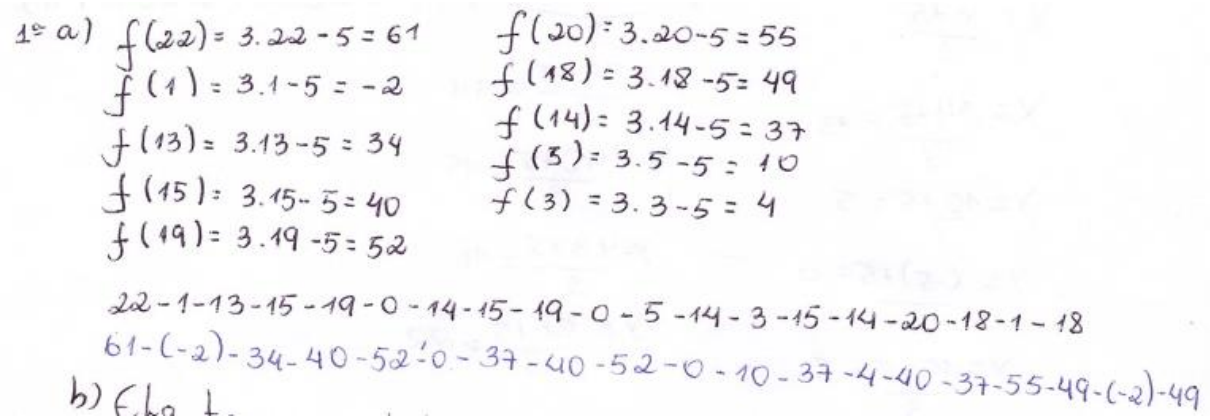


Figura 18: Resolução do Grupo1 para o item "a" da Atividade 1
Fonte: Do Autor

Todos os grupos conseguiram resolver este item corretamente, da forma como havíamos estipulado.

O objetivo do item "b" era testar se a ideia central do processo de decodificação para esta atividade havia sido assimilada. A descrição do passo a passo para a decodificação de uma mensagem nestes moldes não ficou bem clara na resolução dos grupos mas os conceitos matemáticos envolvidos foram determinados de forma consistente, como podemos ver nas resoluções dos grupos 1 e 5 (Figura 19: Resolução dos Grupos 5 e 1 para o item "b" da Atividade 1).

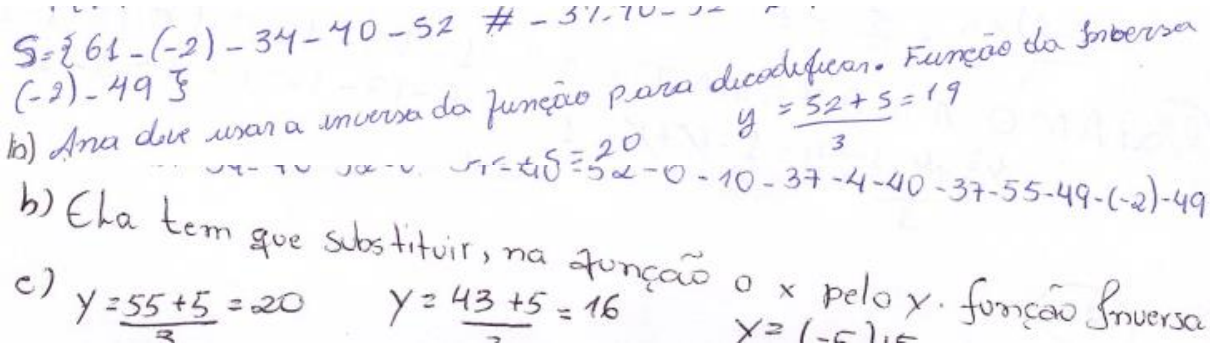


Figura 19: Resolução dos Grupos 5 e 1 para o item "b" da Atividade 1
Fonte: Do Autor

O item "c" consistia na prática do que se explicou com palavras no item "b", ou seja, os alunos receberam uma sequência numérica codificada e deveriam decodificá-la. O objetivo era verificar se o processo de decodificação havia sido assimilado. Após analisar as respostas dos grupos, verificou-se que os grupos 1 e 5 completaram a tarefa. O grupo 3 apresentou apenas o cálculo da função inversa. Os grupos 2 e 4 apresentaram uma "resolução" sem sentido. Veja a resolução de um dos grupos abaixo (Figura 20: Resolução do Grupo 1 para o item "c" da Atividade 1).

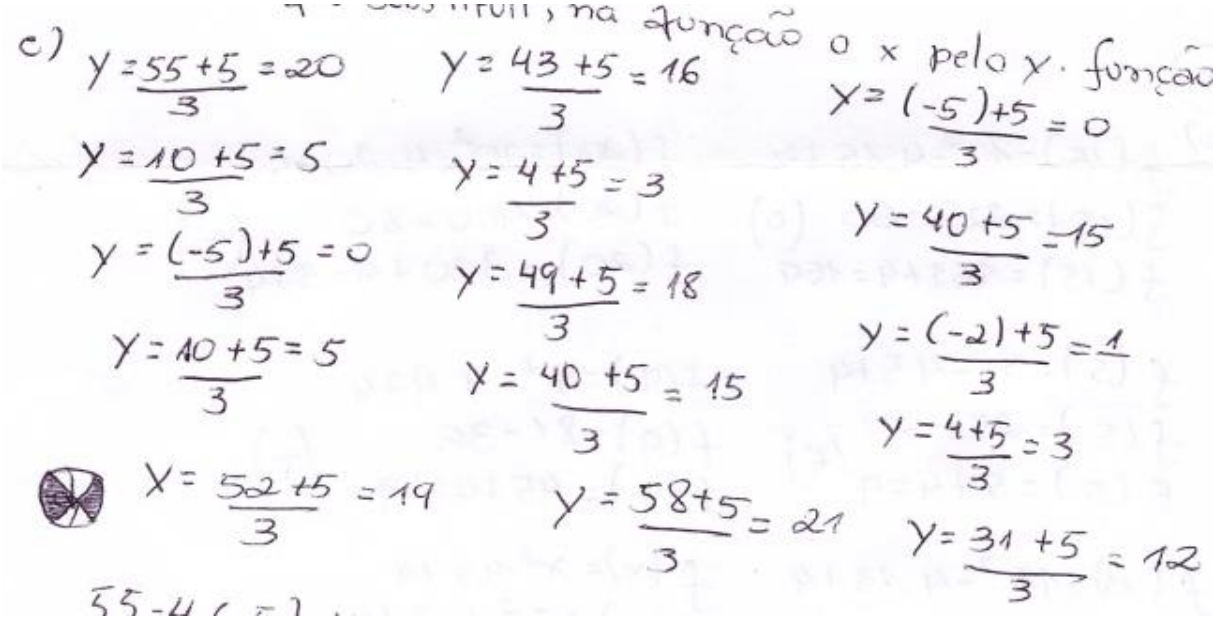


Figura 20: Resolução do Grupo 1 para o item "c" da Atividade 1
Fonte: Do Autor

O objetivo do item "d" era verificar se os alunos haviam entendido que dois pares ordenados eram suficientes para se determinar uma Função Afim. Analisando as respostas dos grupos nota-se que a ideia central foi entendida, pois os grupos 1, 3, 4 e 5 deram uma resposta satisfatória. O grupo 2 apresentou uma resposta incompreensível. Acompanhe abaixo uma das soluções dos alunos (Figura 21: Resolução do Grupo 5 para o item "d" da Atividade 1).

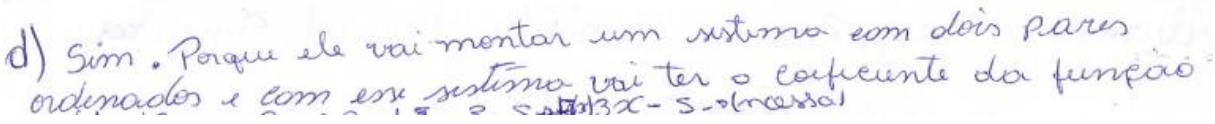


Figura 21: Resolução do Grupo 5 para o item "d" da Atividade 1
Fonte: Do Autor

No item "e" os grupos foram convidados a criar uma mensagem, codificá-la usando usando uma função afim de sua preferência e enviá-la para outro grupo, não esquecendo de fornecer a função cifradora. O objetivo era promover a interação entre os grupos e reforçar o processo de codificação. Os grupos 1 e 5 completaram este item com sucesso. Os grupos 2 e 4 apresentaram a frase e a sequência numérica codificada, mas não as suas funções cifradoras e os respectivos cálculos das imagens. O grupo 3 não apresentou resolução. Observe, na sequência, uma solução dos alunos (Figura 22: Resolução do Grupo 1 para o item "e" da Atividade 1).

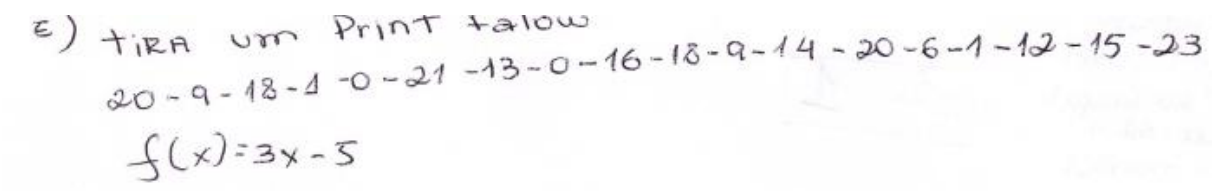


Figura 22: Resolução do Grupo 1 para o item "e" da Atividade 1
Fonte: Do Autor

No item "f" os grupos deveriam decodificar as mensagens recebidas no item anterior. O objetivo era a interação entre os grupos e o reforço do processo de decodificação. Novamente, os grupos 1 e 5 completaram esta tarefa com sucesso. Os grupos 2, 3 e 4 não apresentaram solução para esta tarefa. Veja uma solução de um dos grupos (Figura 23: Resolução do Grupo 5 para o item "f" da Atividade 1).

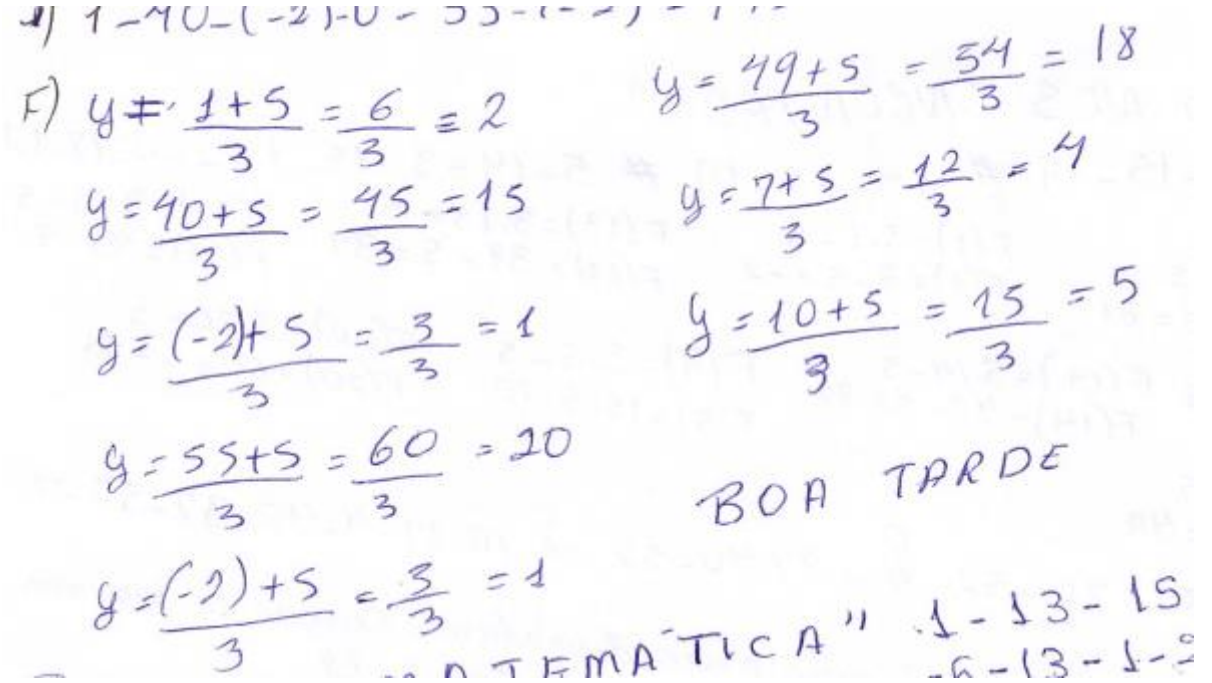


Figura 23: Resolução do Grupo 5 para o item "f" da Atividade 1
Fonte: Do Autor

No transcorrer da Atividade 2 (Criptografando com Função Quadrática), no item "a", depois de terem atribuído valores numéricos às letras da frase que desejavam codificar (com o auxílio da tabela alfabeto-numérica fornecida), os alunos realizaram o cálculo das imagens através da função cifradora fornecida. Os grupos 1, 4 e 5 resolveram o item como se esperava (por completo). Os grupos 2 e 6 realizaram a conversão de letras em números, mas não realizaram os cálculos das respectivas imagens. Já o grupo 3 apresentou o cálculo de apenas uma imagem. Veja uma das resoluções (Figura 24: Resolução do grupo 4 para o item "a" da Atividade 2)

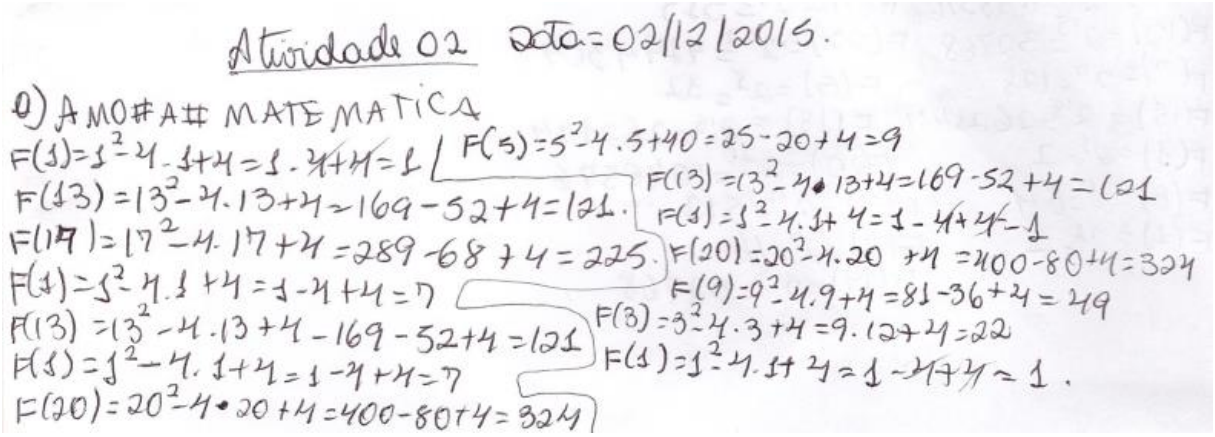


Figura 24: Resolução do grupo 4 para o item "a" da Atividade 2
Fonte: Do Autor

No item "b", os alunos deveriam decodificar uma sequência numérica recebida que foi codificada usando a função cifradora do enunciado, o objetivo era de realizar o cálculo da função inversa (com restrições) e o cálculo das imagens inversas. Ao se analisar a solução dos alunos percebeu-se que o grupo 5 conseguiu completar a tarefa, inclusive contornando o problema das "imagens inversas duplas". Os grupos 1, 2 e 4 conseguiram encontrar a função inversa, calcularam as imagens inversas, mas não conseguiram contornar o problema das "imagens inversas duplas". O grupo 6 apresentou apenas a frase final (decodificada) sem os cálculos necessários para realização de qualquer análise. O grupo 3 apresentou apenas o cálculo da função inversa. Veja uma das resoluções (Figura 25: Resolução do grupo 5 para o item "b" da Atividade 2).

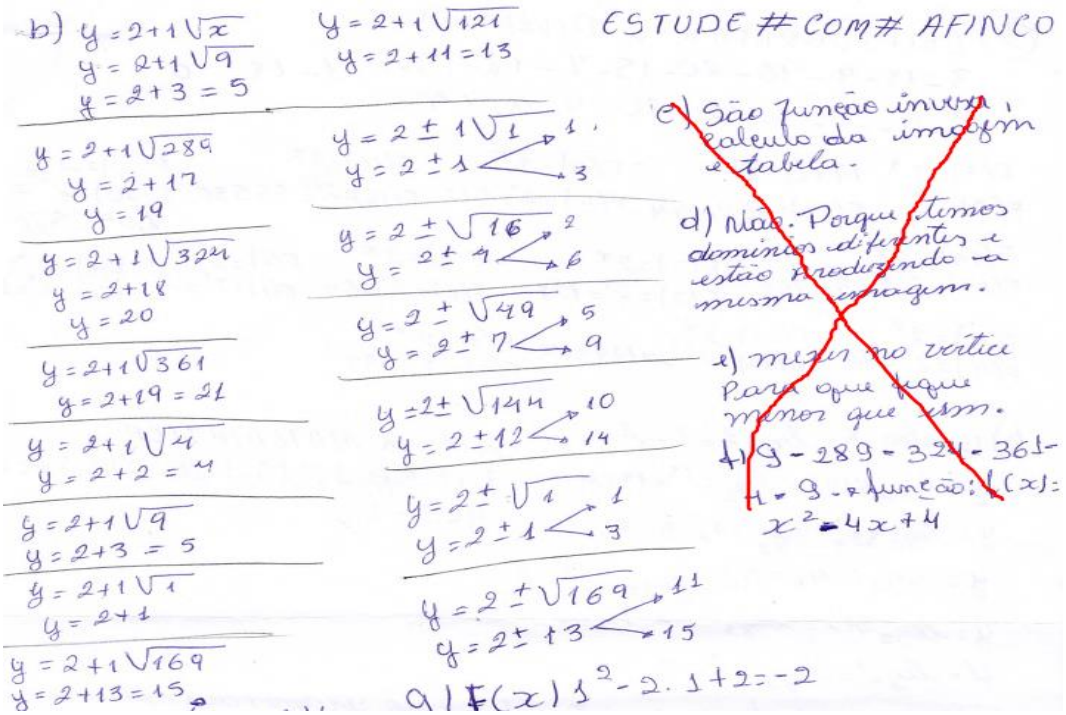


Figura 25: Resolução do grupo 5 para o item "b" da Atividade 2
Fonte: Do Autor

No item “c” os alunos eram convidados a citar quais os conceitos matemáticos envolvidos na resolução do item anterior. O objetivo era de estabelecer uma conexão visível entre os conceitos matemáticos trabalhados e a resolução da atividade. Analisando-se as resoluções vemos que os grupos 1, 2 e 3 citaram apenas a função inversa. O grupo 4 citou o cálculo de imagens inversas. O grupo 6 citou apenas o uso da tabela de conversão alfabeto-numérica. Já o grupo 5 citou a função inversa, cálculo das imagens inversas e fez uso da tabela de conversão alfabeto-numérica, fornecendo uma resposta satisfatória. Veja uma das soluções (Figura 26: Resolução do grupo 5 para o item “c” da Atividade 2).

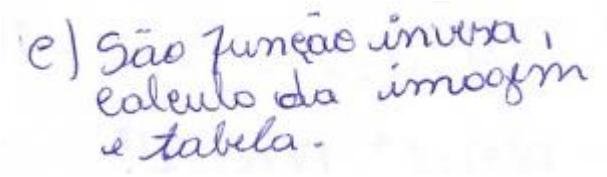


Figura 26: Resolução do grupo 5 para o item “c” da Atividade 2
Fonte: Do Autor

No item “d” foi solicitado aos alunos que dissessem se a função cifradora escolhida $f(x)=x^2-4x+4$ foi uma boa escolha e por quê. O objetivo era mostrar aos alunos que para se ter uma função inversa de uma função quadrática era preciso restringir seu domínio e contra-domínio. Os grupos 1, 2, 4, 5 e 6 responderam que a função cifradora não havia sido uma boa escolha e citaram o fato dela ter fornecido imagens iguais para valores do domínio diferentes. Apenas o grupo 3 disse que não, mas não soube explicar o porquê. Vale ressaltar que neste item foi necessário a intervenção do professor/aplicador com repetição de conceitos envolvidos e resolução de exemplos, pois os alunos não haviam entendido bem o que se pretendia. Acompanhe uma das soluções (Figura 27: Resolução do grupo 1 para o item “d” da Atividade 2).

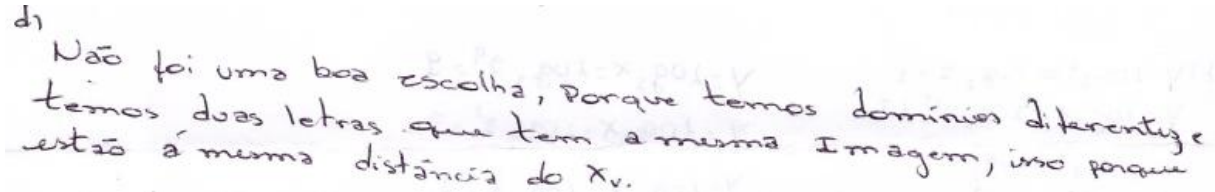


Figura 27: Resolução do grupo 1 para o item “d” da Atividade 2
Fonte: Do Autor

O item “e” era para que os alunos citassem como resolver o problema identificado no item “d”, uma vez que nosso domínio era fixo ($D(f)=\{x\in N\,|\,1\le x\le 26\}$). O grupo 5 relatou que deveria se deslocar o vértice da párabola de forma que o $x_v<1$. O grupo 6 falou em deslocar o vértice da parábola, mas não disse como. O grupo 4 falou em deslocar a parábola para a esquerda na direção do eixo x. Os grupos 1 e 2 falaram em alterar o valor do

coeficiente “b” para que este ficasse positivo (apesar de terem se atrapalhado um pouco com as palavras). O grupo 3 citou uma troca de valor (creio que seria para o coeficiente “b”) mas se atraplahou e a resposta ficou ininteligível. Veja uma das soluções (Figura 28: Resolução do grupo 4 para o item “e” da Atividade 2).

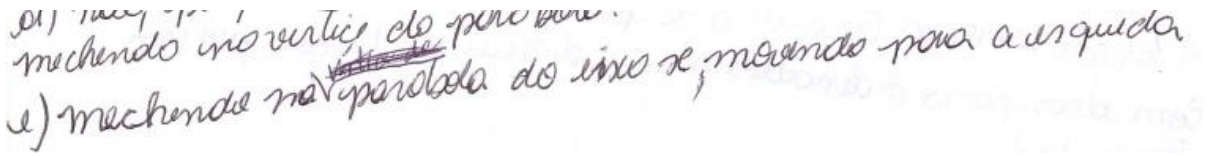


Figura 28: Resolução do grupo 4 para o item “e” da Atividade 2
Fonte: Do Autor

No item “f” os alunos deveriam criar uma mensagem, criptografá-la usando uma função quadrática qualquer e enviá-la a outro grupo. O objetivo era promover a interação entre os grupos e reforçar o processo de cifragem por este método, bem como os conteúdos relacionados. Os grupos 4 e 6 não apresentaram suas soluções para esta tarefa. O grupo 1 apresentou sua frase e a correspondente sequência numérica criptografada, mas se esqueceu de apresentar a função cifradora. O grupo 2 forneceu apenas uma sequência numérica (suponho que seja a sequência cifrada de sua frase). Os grupos 3 e 5 forneceram função cifradora e sequência cifrada, mas se esqueceram das suas frases (o que não é muito relevante). Observe uma das soluções (Figura 29: Solução do grupo 3 para o item “f” da Atividade 2).

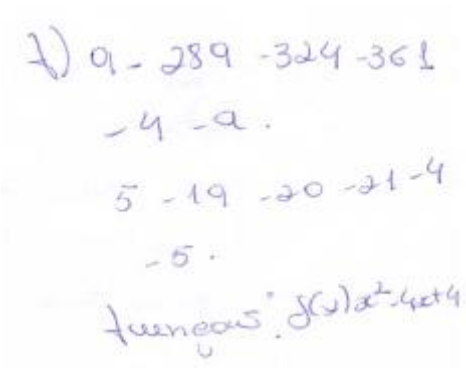


Figura 29: Solução do grupo 3 para o item “f” da Atividade 2
Fonte: Do Autor

No item “g” os alunos deveriam decodificar as frases recebidas no item anterior. O objetivo era promover a interação entre os grupos e reforçar o processo de decifragem por este método, bem como os conteúdos relacionados. Os grupos 1 e 5 apresentaram os cálculos das imagens inversas e a frase decodificada. O grupo 3 apresentou apenas a frase decodificada. Os grupos 2, 4 e 6 não apresentaram solução para este item. Veja (Figura 30: Solução do grupo 1 para o item “g” da Atividade 2).

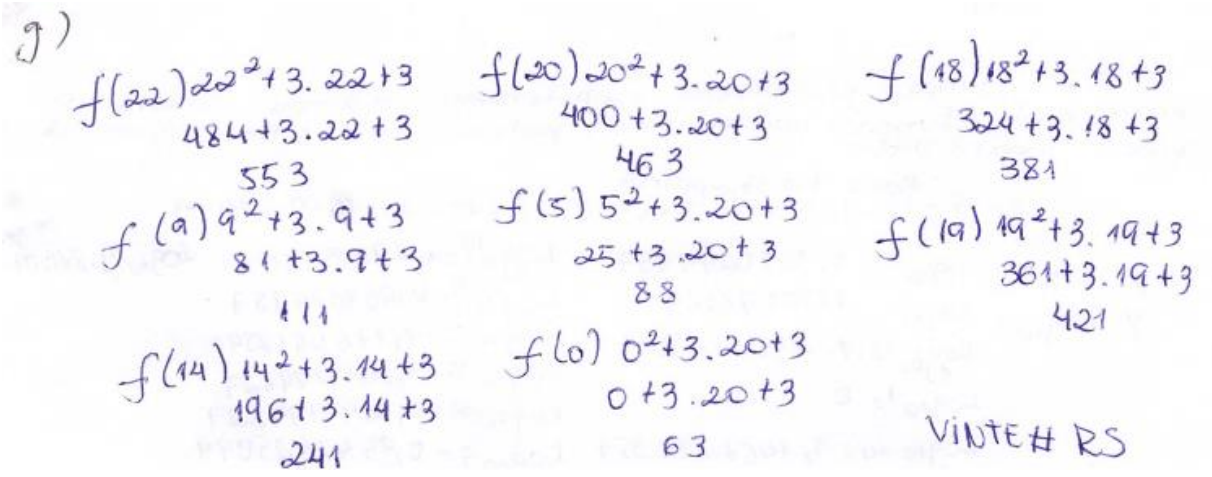


Figura 30: Solução do grupo 1 para o item "g" da Atividade 2
Fonte: Do Autor

Durante a Atividade 3 (Criptografando com Função Exponencial), no item "a", os alunos foram desafiados a codificar uma mensagem usando a função exponencial $f(x)=2^x$ como função cifradora, eles fizeram a conversão de letras da frase em números com o auxílio da tabela alfabeto-numérica, em seguida, calcularam as imagens dos respectivos valores numéricos. Analisando as respostas dos grupos, percebemos que os grupos 1, 2, 4 e 5 apresentaram soluções satisfatórias com suas respectivas sequências numéricas codificadas e cálculos. Os grupos 3 e 6 apresentaram apenas a sequência numérica codificada. Acompanhe uma das soluções dos alunos (Figura 31: Solução do grupo 2 para o item "a" da Atividade 3).

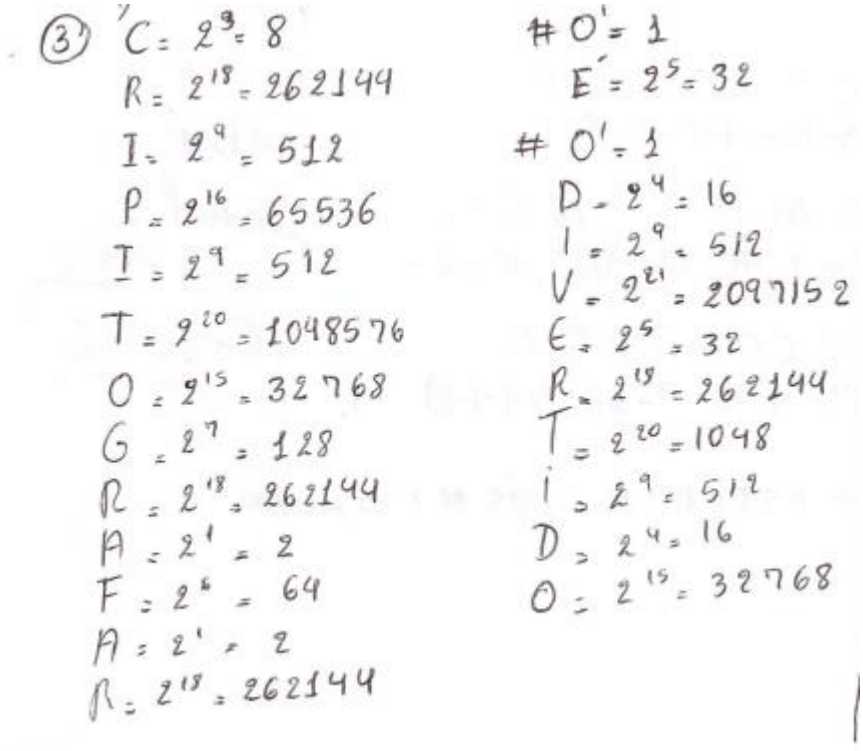


Figura 31: Solução do grupo 2 para o item "a" da Atividade 3
Fonte: Do Auotor

No item “b” os alunos deveriam decodificar uma sequência numérica recebida, codificada pela mesma função cifradora do enunciado. O objetivo era de que eles realizassem o cálculo da função inversa da Exponencial (Função Logarítmica) e de suas respectivas imagens inversas. Os grupos 1, 2, 3, 4 e 5 completaram esta tarefa com sucesso, ou seja, obtiveram a inversa e realizaram os cálculos das imagens inversas. O grupo 6 apresentou apenas a frase decodificada, impossibilitando maiores análises. Observe abaixo uma das soluções dos alunos (Figura 32: Solução do grupo 3 para o item “b” da Atividade 3).

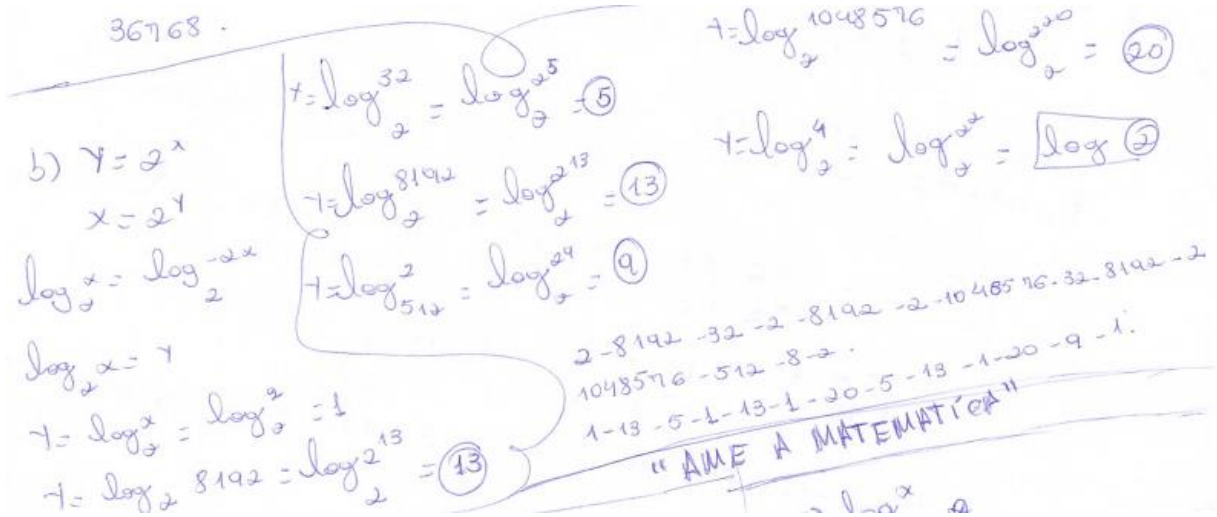


Figura 32: Solução do grupo 3 para o item “b” da Atividade 3
Fonte: Do Autor

Para resolver o item “c” os alunos deveriam citar quais os conceitos matemáticos associados à resolução dos itens anteriores. Os grupos 1, 2, 4 e 5 deram respostas mais completas citando função exponencial e potenciação para a codificação e, função inversa e propriedades de logaritmos para a decodificação. Os grupos 3 e 6 deram respostas menos completas. Veja uma das soluções (Figura 33: Solução do grupo 2 para o item “c” da Atividade 3).

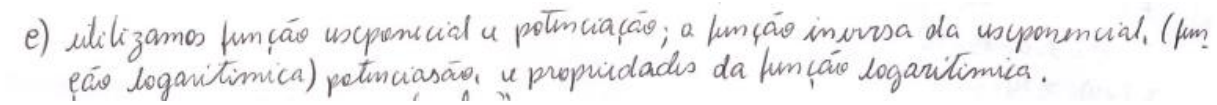


Figura 33: Solução do grupo 2 para o item “c” da Atividade 3
Fonte: Do Autor

No item “d” os alunos deveriam criar uma mensagem, codificá-la usando a função codificadora $f(x)=\log x$ e enviá-la para outro grupo de sua escolha. O objetivo era de estimular a interação entre os grupos e desenvolver a capacidade de codificar usando a função logarítmica. Os grupos 1, 2 e 3 apresentaram suas frases e os respectivos cálculos de suas imagens para codificá-las. O grupo 5 apresentou a frase e a sequência numérica codificada mas não apresentou os cálculos das imagens. O grupo 4 apresentou apenas uma sequência

numérica. O grupo 6 não apresentou solução para esta tarefa. Veja uma das soluções dos alunos (Figura 34: Solução do grupo 1 para o item “d” da Atividade 3).

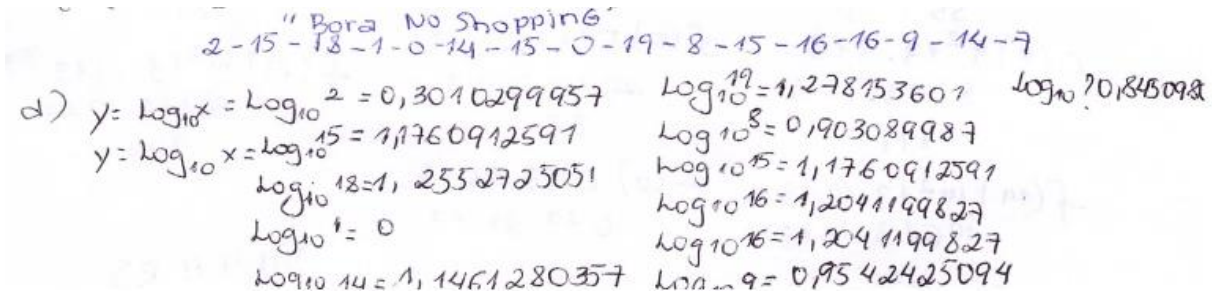


Figura 34: Solução do grupo 1 para o item “d” da Atividade 3
Fonte: Do Autor

Para a resolução do item “e” o aluno deveria decodificar a sequência numérica criptografada recebida no item anterior. O objetivo era de estimular a curiosidade dos alunos e reforçar os conceitos matemáticos envolvidos na resolução. Os grupos 3 e 5 apresentaram apenas a frase decodificada. O grupo 4 apresentou os cálculos das imagens inversas, mas não fez a correspondência alfabeto-numérica para encontrar a frase correspoondente. Os grupos 1, 2 e 6 não apresentaram solução para este item. Acompanhe uma das soluções dos alunos (Figura 35: Solução do grupo 4 para o item “e” da Atividade 3).

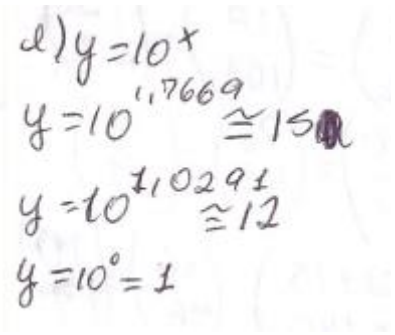


Figura 35: Solução do grupo 4 para o item “e” da Atividade 3
Fonte: Do Autor

No transcorrer da Atividade 4 (Criptografando com Matrizes), no item “a” os alunos deveriam cifrar uma mensagem dada. O objetivo era de mostrar como o produto de matrizes pode ser usado para criptograr mensagens. Após realizarem a conversão das letras em números através da tabela de correspondência alfabeto-numérica, os alunos procederam a resolução deste item. Todos os grupos realizaram esta tarefa de modo satisfatório, ou seja, realizaram o produto da matriz chave pela matriz mensagem, obtendo a matriz código ao final do processo. Veja a solução de um dos grupos (Figura 36: Solução do grupo 6 para o item “a” da Atividade 4).

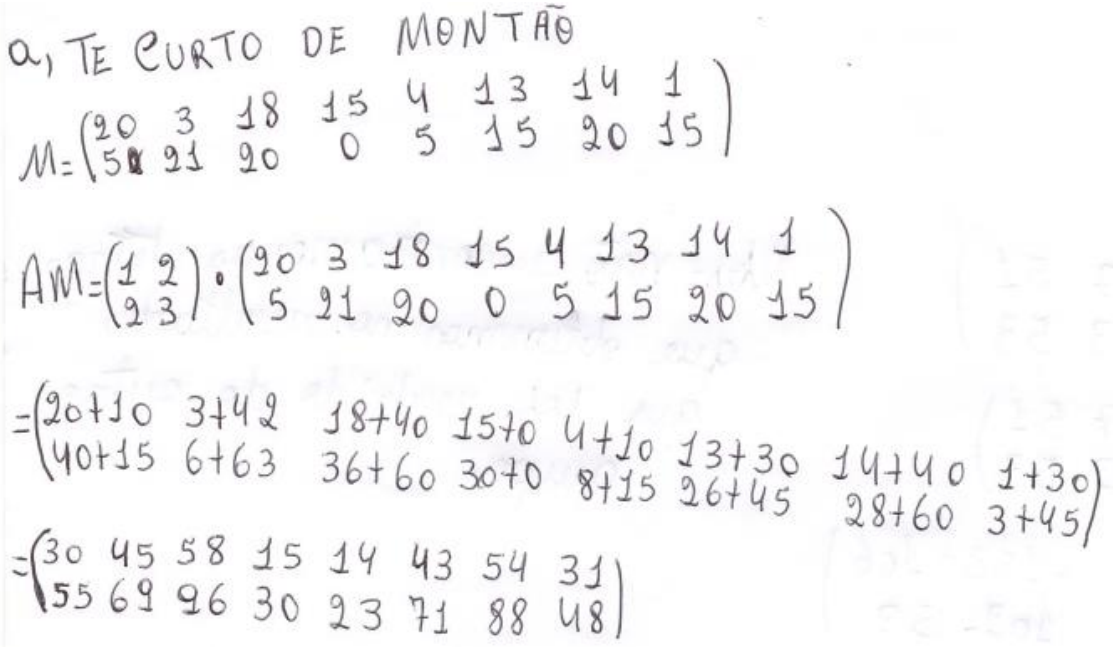


Figura 36: Solução do grupo 6 para o item "a" da Atividade 4
Fonte: Do Autor

Na resoluçao do item "b" os alunos deveriam citar qual o passo a passo para decodificar a mensagem do item anterior, também deveriam citar quais os conceitos matemáticos relacionados ao processo de decodificar uma mensagem nestes parâmetros. O objetivo era verificar se os alunos haviam entendido o processo de decodificação. Os grupos 1, 2 e 5 completeram esta tarefa, isto é, citaram o procedimento para decodificar a mensagem e também a matriz inversa e o produto de matrizes. Os grupos 3 e 4 citaram apenas os conteúdos associados (matriz inversa e produto de matrizes). O grupo 6, por sua vez, citou apenas que deveria ser usada a matriz decodificadora $\boldsymbol{A^{-1}}$. Acompanhe a solução de um dos grupos (Figura 37: Resolução do grupo 1 para o item "b" da Atividade 4).

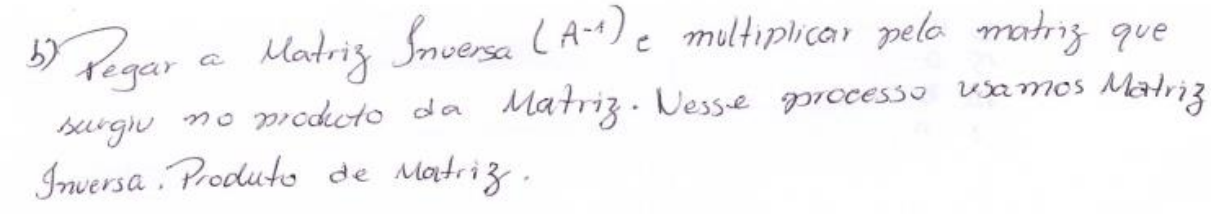


Figura 37: Resolução do grupo 1 para o item "b" da Atividade 4
Fonte: Do Autor

No item "c" os alunos deveriam decodificar uma sequência numérica codificada recebida. O objetivo era trabalhar o produto da matriz inversa $\boldsymbol{A^{-1}}$ pela matriz codificada $\boldsymbol{AM}$. Os grupos 1, 2, 5 e 6 realizaram com o produto de matrizes e apresentaram a matriz mensagem M, ficou faltando apenas realizar a conversão dos números da matriz $\boldsymbol{M}$ em letras através da tabela de conversão alfabeto-numérica. O grupo 3 realizou esta tarefa em sua

totalidade. O grupo 4 não apresentou solução para este item. Observe a solução de um dos grupos (Figura 38: Solução do grupo 3 para o item "c" da Atividade 4).

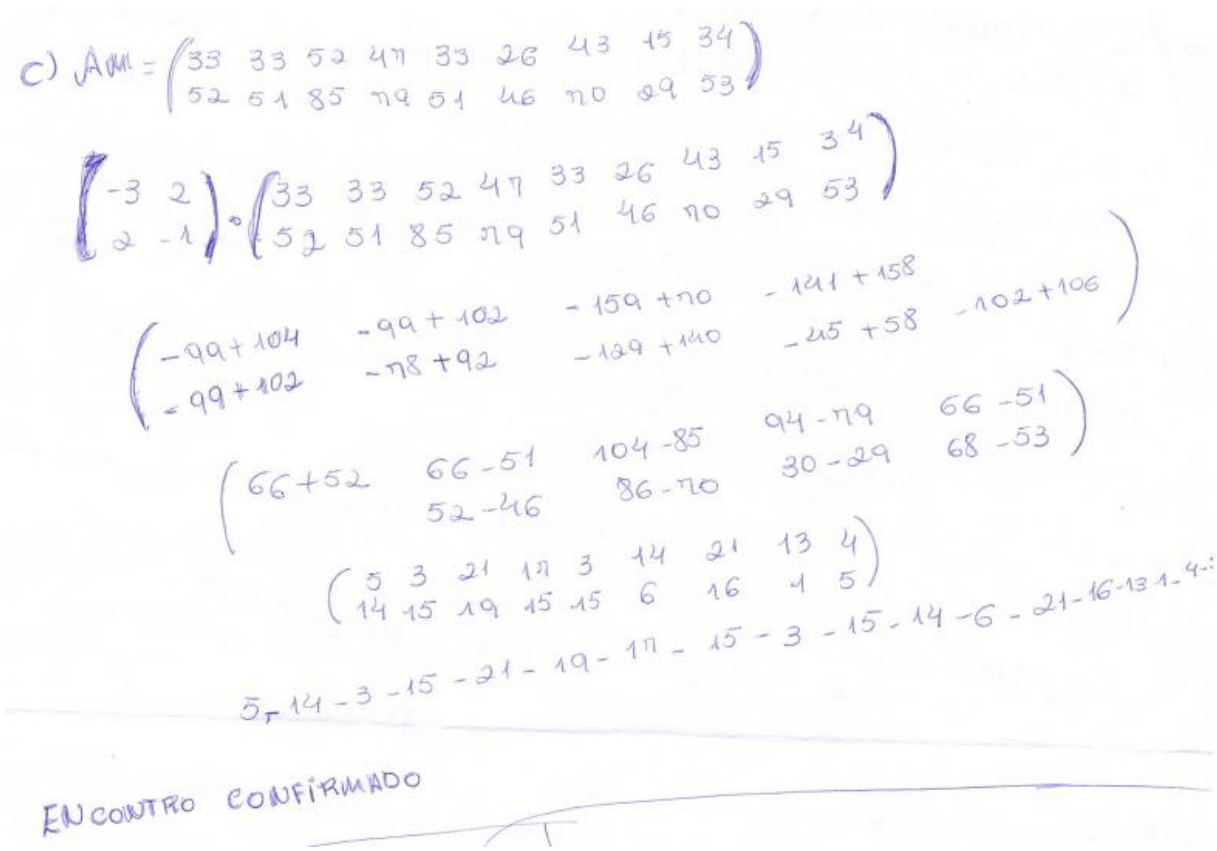


Figura 38: Solução do grupo 3 para o item "c" da Atividade 4
Fonte: Do Autor

No item "d" os alunos deveriam dizer se para o caso em que uma pessoa tivesse posse da sequência numérica do item anterior e da tabela de conversão alfabeto-numérica, seria ela capaz de decodificar a mensagem. O objetivo era reforçar a importância da matriz inversa $\boldsymbol{A^{-1}}$ para a decodificação de mensagens por este processo. Os grupos 1, 2, 3, 4 e 5 apresentaram soluções satisfatórias. Apenas o grupo 6 não apresentou solução para este item. Veja uma das soluções dos alunos (Figura 39: Solução do grupo 2 para o item "d" da Atividade 4).

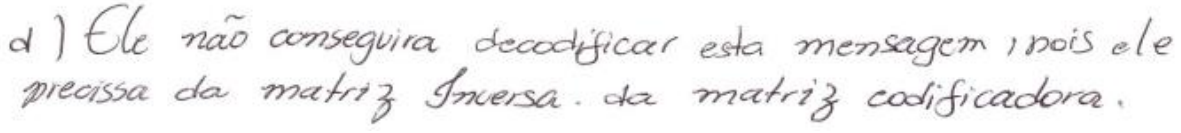


Figura 39: Solução do grupo 2 para o item "d" da Atividade 4
Fonte: Do Autor

Para resolver o item "e" os alunos deveriam criar uma mensagem, usando uma matriz 2x2 cifradora de livre escolha (desde que tenha inversa) e enviá-la para outro grupo, não esquecendo de fornecer a matriz cifradora ao grupo destinatário da mensagem. O objetivo

era promover a interação entre os grupos e reforçar o processo de codificação utilizando este método. Os grupos 1 e 5 apresentaram respostas satisfatórias. Os grupos 2, 3, 4 e 6 não apresentaram solução por escrito para esta tarefa, embora no momento da realização das atividades tenha sido observada a troca de mensagens entre os grupos. Acompanhe a solução de um dos grupos (Figura 40: Solução do grupo 1 para o item "e" da Atividade 4).

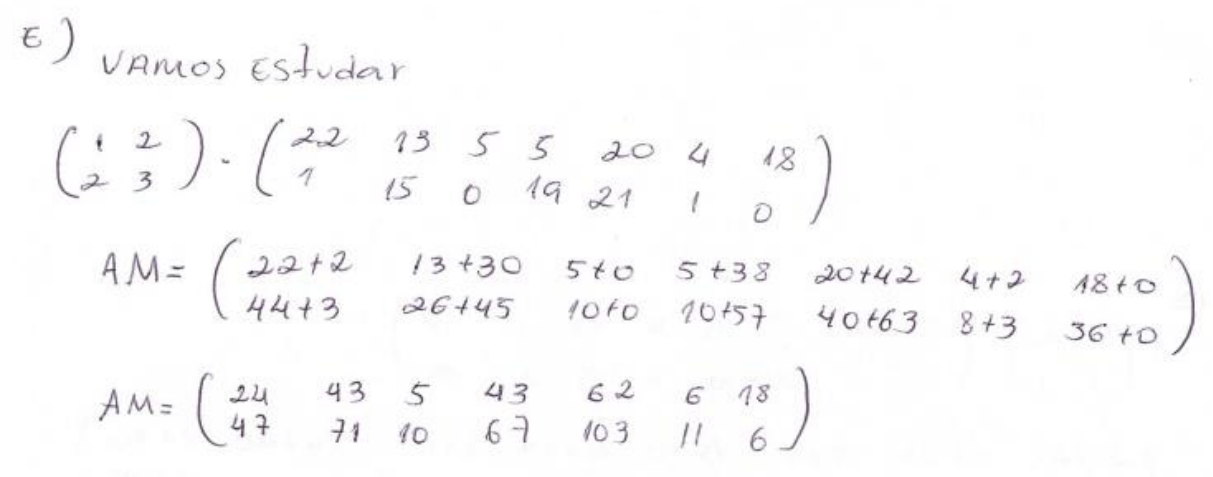


Figura 40: Solução do grupo 1 para o item "e" da Atividade 4
Fonte: Do Autor

No item "f" os alunos deveriam decodificar a mensagem recebida no item anterior. O objetivo era estimular a curiosidade dos alunos e reforçar o processo de decodifiação. Os grupos 1 e 5 apresentaram suas soluções completas. O grupo 6 apresentou os cálculos, mas não obteve correspondência alfabética. Os grupos 2, 3 e 4 não apresentaram solução para esta tarefa. Observe, na sequência, a solução de um dos grupos (Figura 41: Solução do grupo 5 para o item "f" da Atividade 4).

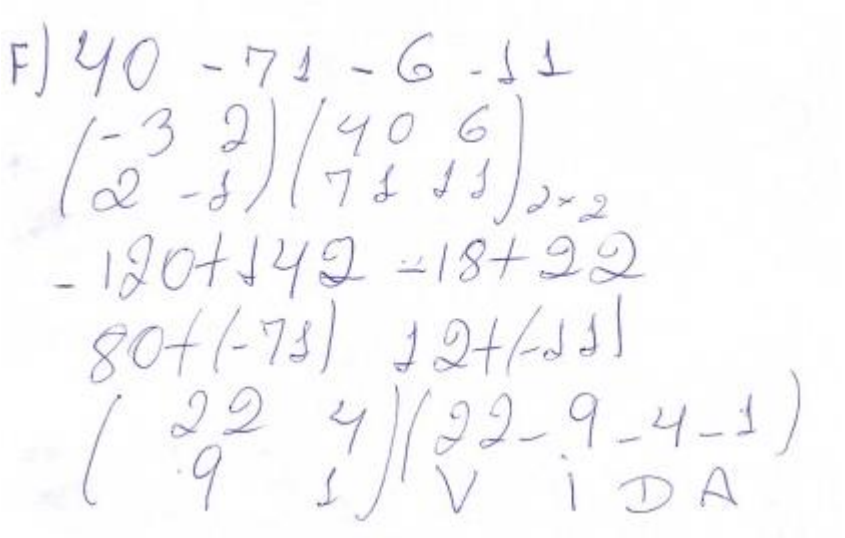


Figura 41: Solução do grupo 5 para o item "f" da Atividade 4
Fonte: Do Autor

Antes da Atividade 5 (Criptografando com Cifra de Hill) foram apresentados alguns conceitos de Aritmética Modular e, forneceu-se uma nova tabela de conversão alfabeto-numérica e uma tabela de recíprocos módulo 26 para facilitar os cálculos. No item "a" os alunos foram convocados a codificar a frase dada no enunciado. O objetivo era de aplicar o processo de codificação pelo método de Hill e, consequentemente, o produto de matrizes. Primeiramente, os alunos fizeram a conversão das letras da frase em números com o auxílio da nova tabela de conversão alfabeto-numérica, em seguida, procederam a separação em pares para formar os vetores mensagem ($\boldsymbol{p_i}$), logo depois, foi realizado o produto da matriz codificadora $\boldsymbol{A}$ por cada um dos vetores mensagem $\boldsymbol{p_i}$, obtendo o vetor codificado $\boldsymbol{Ap_i}$. Em seguida, os alunos tomaram a congruência módulo 26 de cada um dos números dos vetores decodificados. Os grupos 2, 4, 5 e 6 apresentaram soluções completas. O grupo 3 apresentou os vetores codificados e tomaram as congruências módulo 26 dos números de cada vetor, mas não fizeram a conversão dos números em letras do nosso alfabeto. O grupo 1 não apresentou solução para este item. Veja a solução de um dos grupos (Figura 42: Solução do grupo 4 para o item "a" para a Atividade 5).

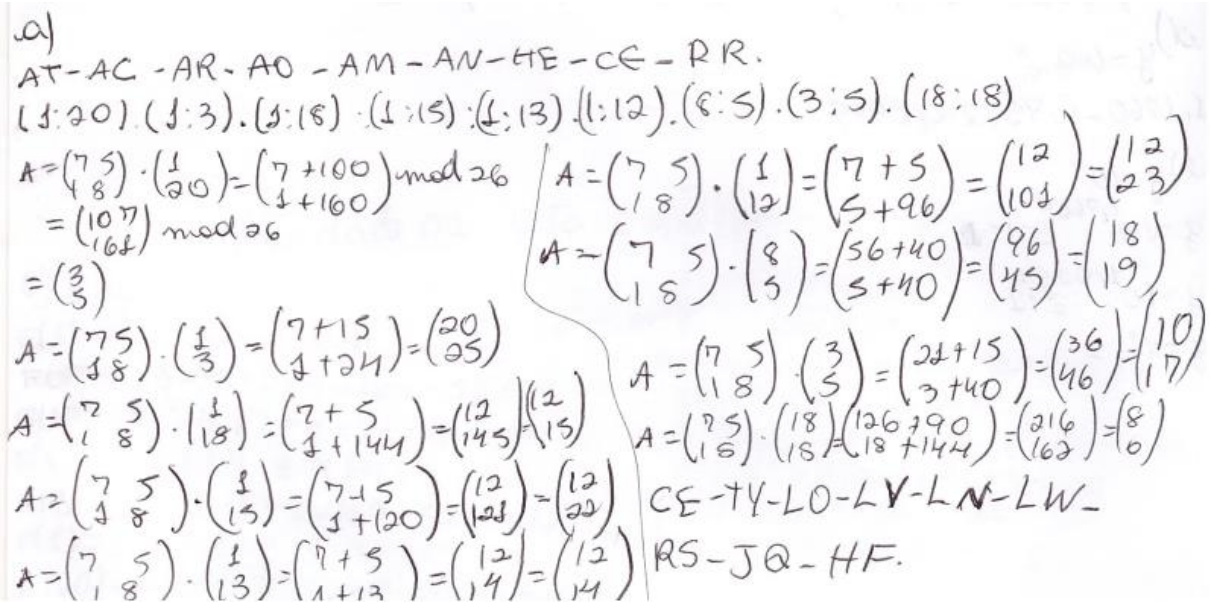


Figura 42: Solução do grupo 4 para o item "a" para a Atividade 5
Fonte: Do Autor

No item "b" os alunos deveriam descrever os procedimentos para decodificar a mensagem do item "a" e calcular a matriz inversa módulo 26 da matriz $\boldsymbol{A}$. O objetivo era verificar se o processo de decodificação havia sido compreendido e efetuar o cálculo da inversa módulo 26 da matriz codificadora. Os grupos 5 e 6 apresentaram soluções completas. O grupo 2 descreveu apenas o processo para decodificação da mensagem. Os grupos 1, 3 e 4

não apresentaram solução para este item. Acompanhe uma das soluções dos alunos (Figura 43: Solução do grupo 5 para o item “b” da Atividade 5).

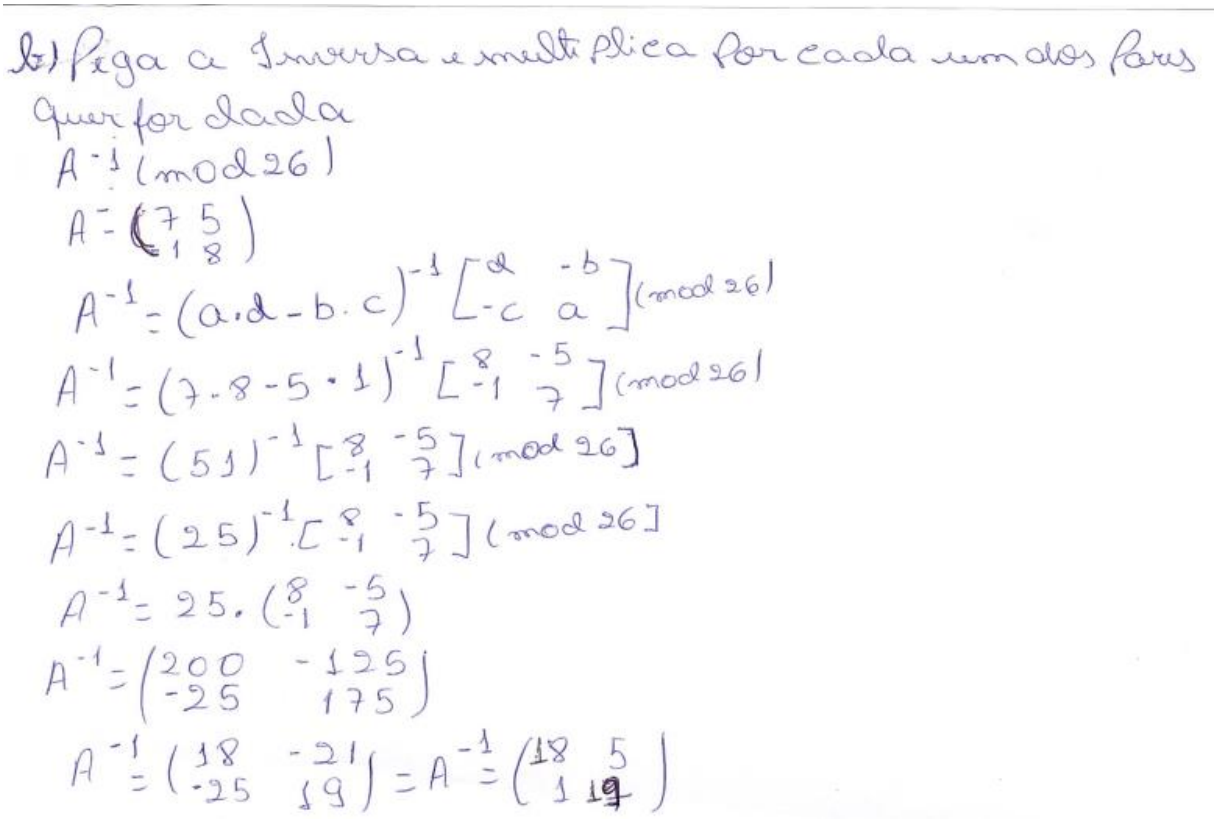


Figura 43: Solução do grupo 5 para o item “b” da Atividade 5
Fonte: Do Autor

No item “c” os alunos foram conclamados a citar quais os conceitos matemáticos envolvidos nos processos de codificação e de decodificação da mensagem dada no enunciado. O objetivo era verificar se os alunos conseguiam perceber a aplicação dos conceitos matemáticos nos processos. O grupo 5 citou matriz inversa módulo 26 e congruência módulo 26. O grupo 3 citou matriz inversa somente. Os demais grupos não apresentaram solução para este item. Observe, a seguir, uma das soluções de um dos grupos (Figura 44: Solução do grupo 5 para o item “c” da Atividade 5).

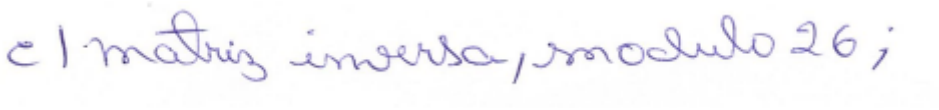


Figura 44: Solução do grupo 5 para o item “c” da Atividade 5
Fonte: Do Autor

No item “d” os alunos deveriam criar uma mensagem curta, criptografá-la usando a matriz ***A*** dada no enunciado e enviá-la a outro grupo de sua preferência. O objetivo era promover a interação entre os grupos e reforçar o processo de codificação. Os grupos 2 e 5

apresentaram soluções completas. Os demais grupos não apresentaram solução para este item. Veja uma das soluções (Figura 45: Solução do grupo 2 para o item “d” da Atividade 5).

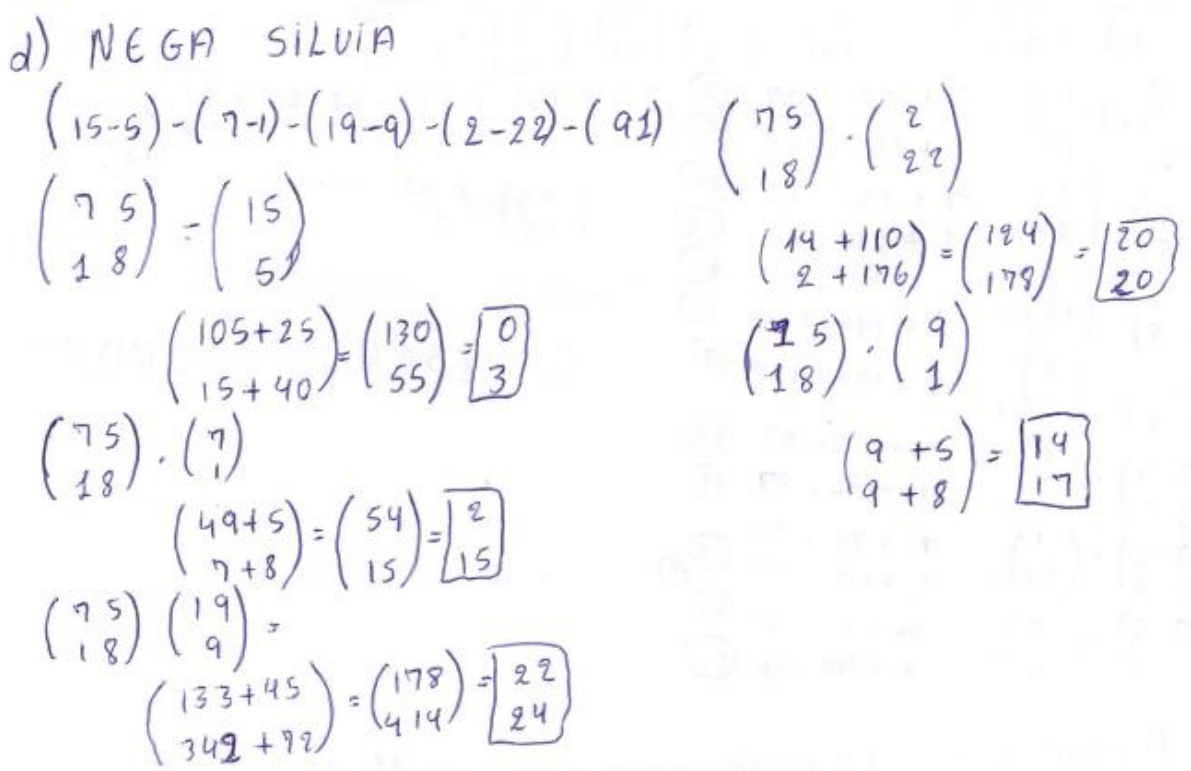


Figura 45: Solução do grupo 2 para o item “d” da Atividade 5
Fonte: Do Autor

Para solucionar o item “e” os alunos deveriam decodificar a mensagem recebida no item anterior. O objetivo era estimular a curiosidade dos alunos e reforçar o processo de decodificação. O grupo 5 apresentou uma solução com letras que não correspondiam a uma frase inteligível. O grupo 2 apresentou uma sequência numérica, mas sem aplicar a congruência módulo 26 e sem fazer a conversão dos números em letras. Os demais grupos não apresentaram solução para este item. Acompanhe, na sequência, duas soluções dos alunos (Figura 46: Soluções dos grupos 2 e 5, respectivamente, para o item “e” da Atividade 5).

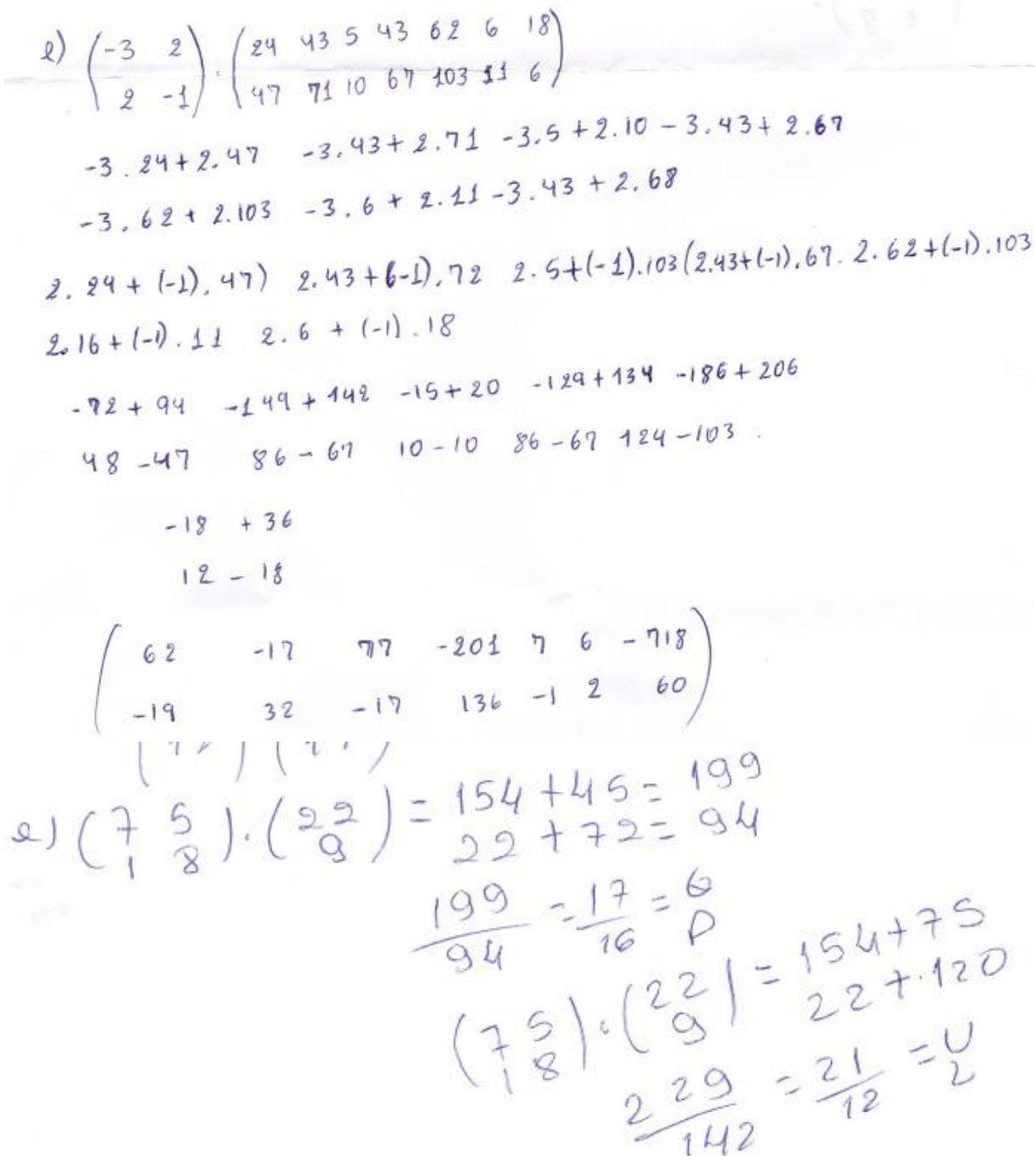


Figura 46: Soluções dos grupos 2 e 5, respectivamente, para o item "e" da Atividade 5
Fonte: Do Autor

Para uma melhor compreensão do desempenho dos grupos na resolução das atividades, desenvolvemos a Tabela 14: Desempenho dos Grupos em Cada Item das Atividades, que resume como foi o desempenho de cada grupo na resolução de cada item, em cada uma das atividades. Nela estão atribuídos conceitos às resoluções apresentadas, para cada item, por cada grupo: resolução total; resolução parcia; não realizado; resolução imcompreensível.

Atividade	GRUPO 1	GRUPO 2	GRUPO 3	GRUPO 4	GRUPO 5	GRUPO 6
1a	Resolução Total	Resolução Parcial	Resolução Parcial	Resolução total	Resolução total	Não Realizado*
1b	Resolução Total	Resolução Total	Resolução Total	Resolução total	Resolução total	Não Realizado*
1c	Resolução Total	Resolução Incompreensível	Resolução Parcial	Resolução Incompreensível	Resolução total	Não Realizado*
1d	Resolução Total	Resolução Incompreensível	Resolução Total	Resolução total	Resolução total	Não Realizado*
1e	Resolução Total	Resolução Parcial	Não Realizado	Resolução parcial	Resolução total	Não Realizado*
1f	Resolução Total	Não Realizado	Não Realizado	Não Realizado	Resolução total	Não Realizado*
2a	Resolução Total	Resolução Parcial	Resolução Parcial	Resolução Total	Resolução Total	Resolução Parcial
2b	Resolução Parcial	Resolução Parcial	Resolução Parcial	Resolução Parcial	Resolução Total	Resolução Parcial
2c	Resolução Parcial	Resolução Parcial	Resolução Parcial	Resolução Parcial	Resolução Total	Resolução Parcial
2d	Resolução Total	Resolução Total	Resolução Parcial	Resolução Total	Resolução Total	Resolução Total
2e	Resolução Parcial	Resolução Parcial	Resolução Parcial	Resolução Parcial	Resolução Total	Resolução Parcial

2f	Resolução Parcial	Resolução Parcial	Resolução Parcial	Não Realizado	Resolução Total	Não Realizado
2g	Resolução Total	Não Realizado	Resolução Parcial	Não Realizado	Resolução Total	Não Realizado
3a	Resolução Total	Resolução Total	Resolução Parcial	Resolução Total	Resolução Total	Resolução Parcial
3b	Resolução Total	Resolução Total	Resolução Total	Resolução Total	Resolução Total	Resolução Parcial
3c	Resolução Total	Resolução Total	Resolução Parcial	Resolução Total	Resolução Total	Resolução Parcial
3d	Resolução Total	Resolução Total	Resolução Total	Resolução Parcial	Resolução Parcial	Não Realizado
3e	Não Realizado	Não Realizado	Resolução Parcial	Resolução Total	Resolução Parcial	Não Realizado
4a	Resolução Total	Resolução Total	Resolução Total	Resolução Total	Resolução Total	Resolução Total
4b	Resolução Total	Resolução Total	Resolução Parcial	Resolução Parcial	Resolução Total	Resolução Parcial
4c	Resolução Total	Resolução Total	Resolução Total	Não Realizado	Resolução Total	Resolução Total
4d	Resolução Total	Resolução Total	Resolução Total	Resolução Total	Resolução Total	Não Realizado
4e	Resolução Total	Não Realizado	Não Realizado	Não Realizado	Resolução Total	Não Realizado

4f	Resolução Total	Não Realizado	Não Realizado	Não Realizado	Resolução Total	Resolução Parcial
5a	Não Realizado	Resolução Total	Resolução Parcial	Resolução Total	Resolução Total	Resolução Total
5b	Não Realizado	Resolução Parcial	Não Realizado	Não Realizado	Resolução Total	Resolução Total
5c	Não Realizado	Não Realizado	Resolução Parcial	Não Realizado	Resolução Total	Não Realizado
5d	Não Realizado	Resolução Total	Não Realizado	Não Realizado	Resolução Total	Não Realizado
5e	Não Realizado	Resolução Parcial	Não Realizado	Não Realizado	Resolução Parcial	Não Realizado

(*): Não realizado por motivo de ausência

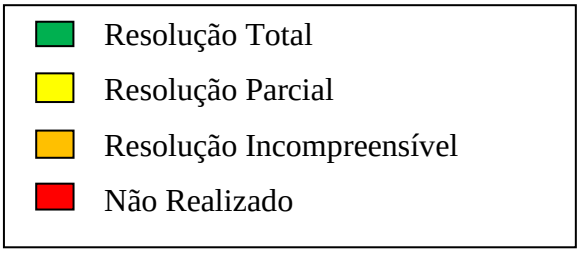


Tabela 14: Desempenho dos Grupos em Cada Item das Atividades
Fonte: Do Autor

Deve-se salientar que durante a aplicação da sequência didática os alunos estiveram mais concentrados nas atividades (pelo menos na maior parte do tempo), diminuindo a ansiedade e as conversas paralelas. Observou-se uma boa discussão em grupo de assuntos relevantes sobre as atividades propostas. Também se observou uma divisão de tarefas dentro dos grupos para otimizar a resolução das tarefas, promovendo, dessa forma, uma boa relação interpessoal dentro dos grupos e entre estes.

Outro fator importante para se citar é que se constatou, através da análise dos dados coletados, que os alunos compreenderam o que se propunha em cada uma das atividades e lograram êxito em suas resoluções (ao menos na grande maioria), mantiveram-se concentrados e demonstraram interesse durante o processo. Vale salientar que os alunos

citaram cansaço ao final da sequência didática, este fato se refletiu na resolução da última atividade que foi a que apresentou menor número de soluções bem sucedidas.

Importante relatar aqui que os alunos foram orientados pelo professor/aplicador a, sempre que surgissem dúvidas, primeiramente, discuti-las em grupo, em seguida, caso não conseguissem solucioná-la dentro do grupo, levar a dúvida ao professor/aplicador para uma discussão mais ampla. No decorrer da aplicação da Atividade 1, os alunos pareceram compreender bem o que cada item solicitava, com exceção do item "d" que abordava a caracterização da função afim pelo conhecimento de dois de seus pares ordenados, eles pareceram não compreender a montagem e tampouco a resolução do sistema linear 2x2.

Durante a resolução do item "b" da Atividade 2, verificou-se uma dificuldade na obtenção da função inversa da função quadrática dada (com domínio e contra-domínio restritos, possibilitando a existência de função inversa), após uma intervenção do professor/aplicador com a resolução de um exemplo, o problema pareceu ter sido resolvido. O problema residia no fato de que alguns valores do domínio apresentavam imagens iguais, devido à escolha da função cifradora, fato que deveria ser trabalhado no item "d". Na resolução do item "d", mesmo após discussão antecipada durante a resolução do item "b", os alunos mostraram dificuldades em resolver o problema, fazendo-se necessária uma nova intervenção por parte do professor/aplicador. Ainda foram observados e relatados pelos alunos dificuldades na resolução do item "e", mesmo sendo uma consequência das intervenções feitas nos itens "b" e "d"; e do item "f", onde os alunos relataram dificuldades para a escolha de uma função quadrática para ser a função cifradora de suas frases.

A atividade 3 proporcionou aos alunos a possibilidade de relacionar função exponencial e função logarítmica como inversas uma da outra. Os alunos apresentaram uma pequena dificuldade, no item "b", em como obter a inversa e as imagens inversas de uma função exponencial, após a intervenção do professor/aplicador o problema foi dirimido. Outras dificuldades relatadas pelos alunos ocorreram durante a resolução dos itens "d" e "e", referiam-se em como obter a inversa da função logarítmica, após uma breve intervenção os alunos compreenderam e resolveram suas atividades.

A atividade 4 foi a que necessitou de menores intervenções, haja vista que eles haviam acabado de estudar o conteúdo com sua professora. Esta atividade proporcionou aos alunos uma revisão das operações com matrizes e cálculo para obtenção da matriz inversa. Comentários adicionais se fizeram necessários apenas para ressaltar a importância da matriz inversa para o processo de decodificação.

A Atividade 5 proporcionou aos alunos a oportunidade de conhecerem conteúdos novos (alguns tópicos de Aritmética Modular). Intervenções se fizeram necessárias em poucas ocasiões, especialmente para a obtenção da inversa módulo 26 da matriz cifradora $\boldsymbol{A}$.

De acordo com a revisão histórica e as atividades desenvolvidas, criou-se uma sequência didática que possibilitou aos alunos conhecer o tema Criptografia através de atividades didáticas envolvendo alguns dos principais conteúdos matemáticos do ensino médio (funções e matrizes), além da introdução de conteúdos ainda desconhecidos pelos alunos (tópicos de Aritmética Modular).

6.5 Análise dos Questionários

Analisando o questionário pré-atividades (Apêndice A), encontramos alguns dados que acreditamos ser importantes compartilhar, por exemplo, a distribuição de idade da turma fica melhor compreendida quando observamos, a seguir, o Gráfico 1: Distribuição etária dos alunos.

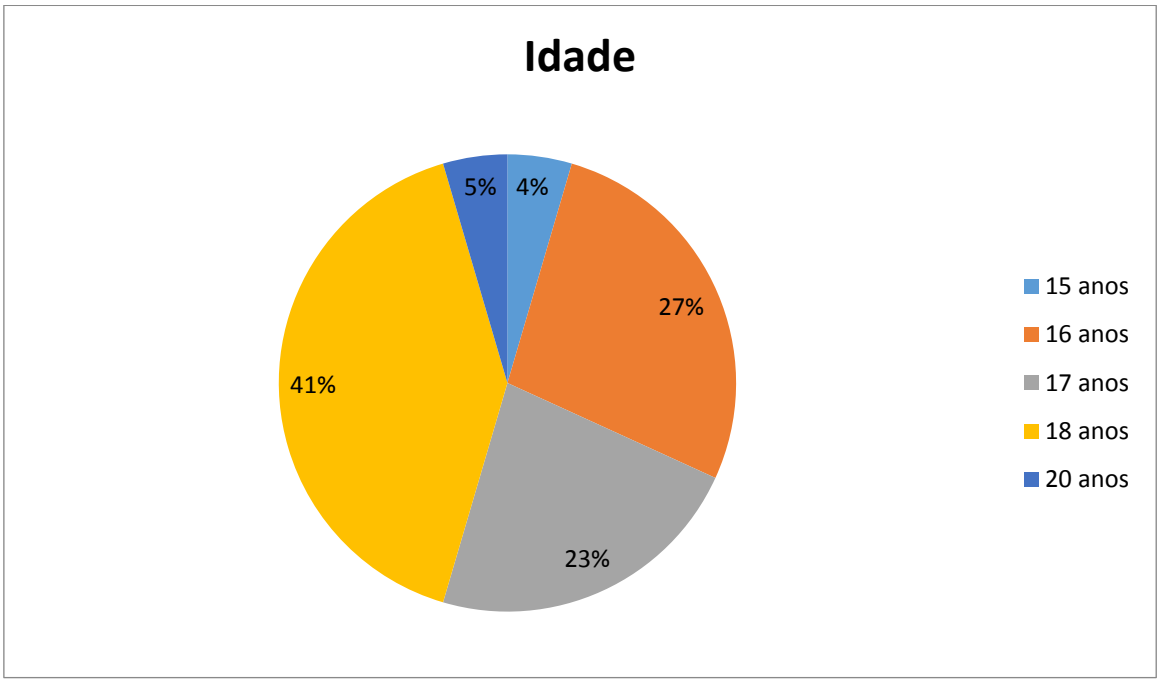


Gráfico 1: Distribuição etária dos alunos
Fonte: Do Autor

Outro dado obtido da análise do questionário pré-atividades é sobre a variável disciplina favorita, observe abaixo (Gráfico 2: Disciplina Favorita) as preferências dos alunos.

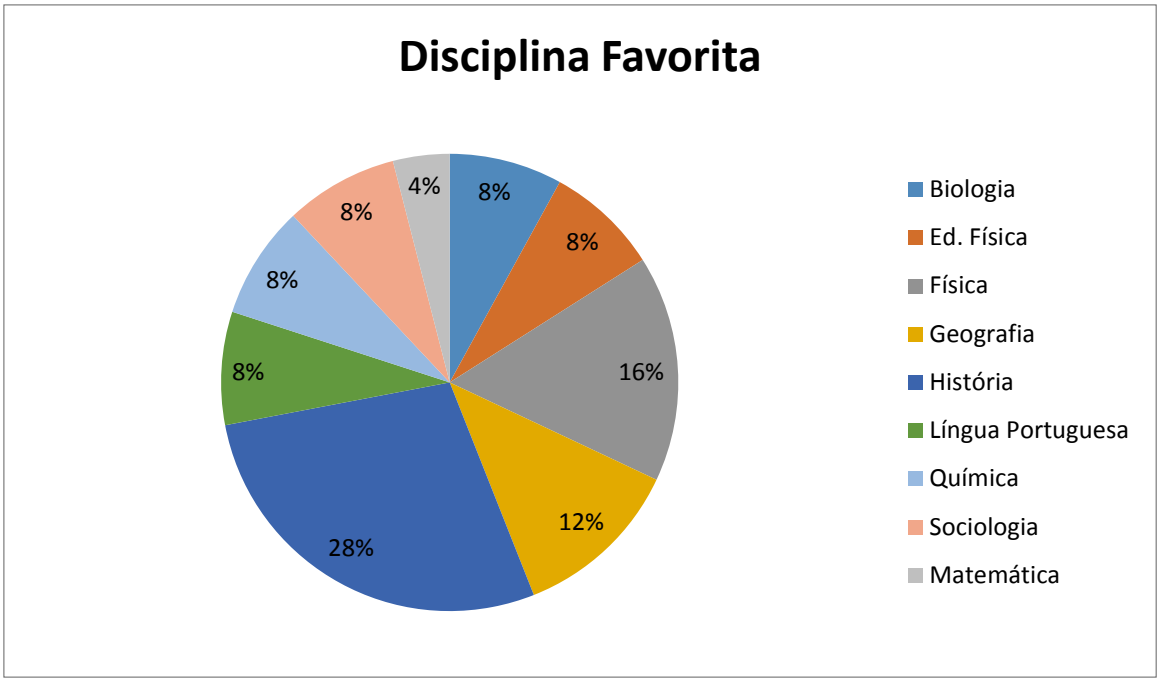


Gráfico 2: Disciplina Favorita
Fonte: Do Autor

Sobre o gráfico acima cabem alguns comentários, três alunos optaram por duas disciplinas, os demais por apenas uma. Causou-nos estranheza o fato de 16% do total ter escolhido Física como disciplina favorita e apenas 4% ter escolhido Matemática, haja vista que são disciplinas afins. Uma explicação plausível reside no fato de que os alunos costumam chamar a disciplina Educação Física de, apenas, Física. Ou, talvez, eles gostem de Física mesmo, fato este que não costuma acontecer muito.

Outra pergunta abordada, no questionário pré-atividades, que achamos importante comentar foi: você exerce atividade remunerada além de estudar? O Gráfico 3: Atividade Remunerada mostra as respostas dadas pelos alunos.

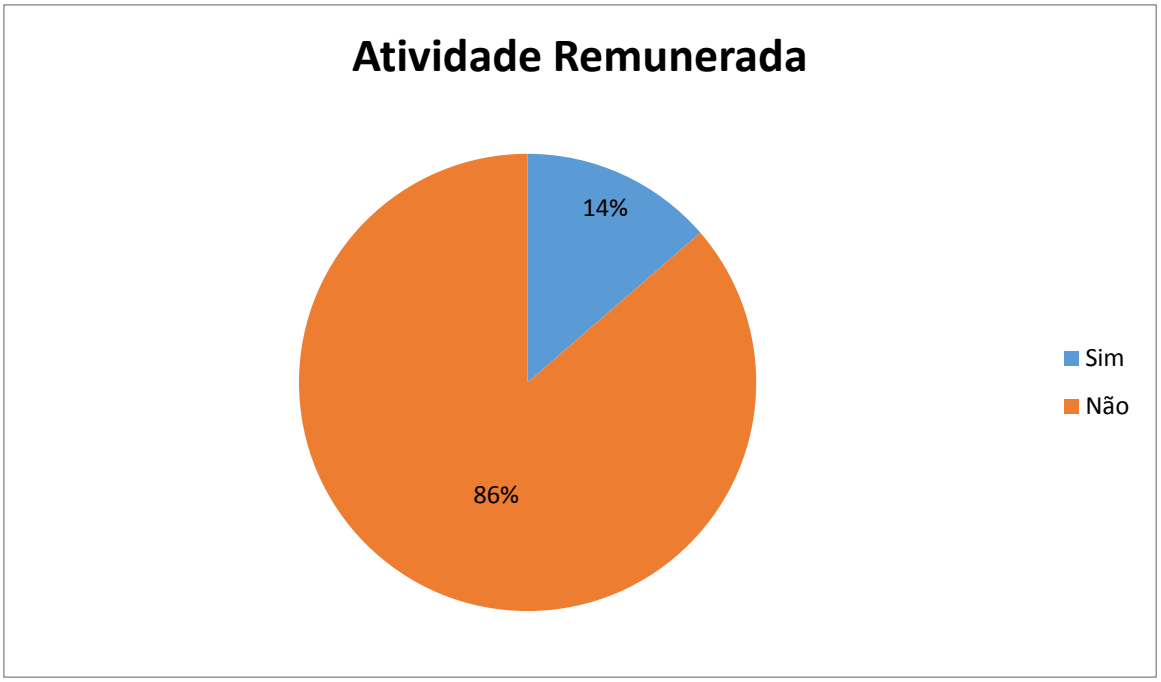


Gráfico 3: Atividade Remunerada
Fonte: Do Autor

O Gráfico 4: "Você Já Repetiu de Ano ou Ficou em Dependência de Estudos?" mostra as respostas dos alunos para a pergunta: você já repetiu algum ano ou ficou em dependência de estudos?

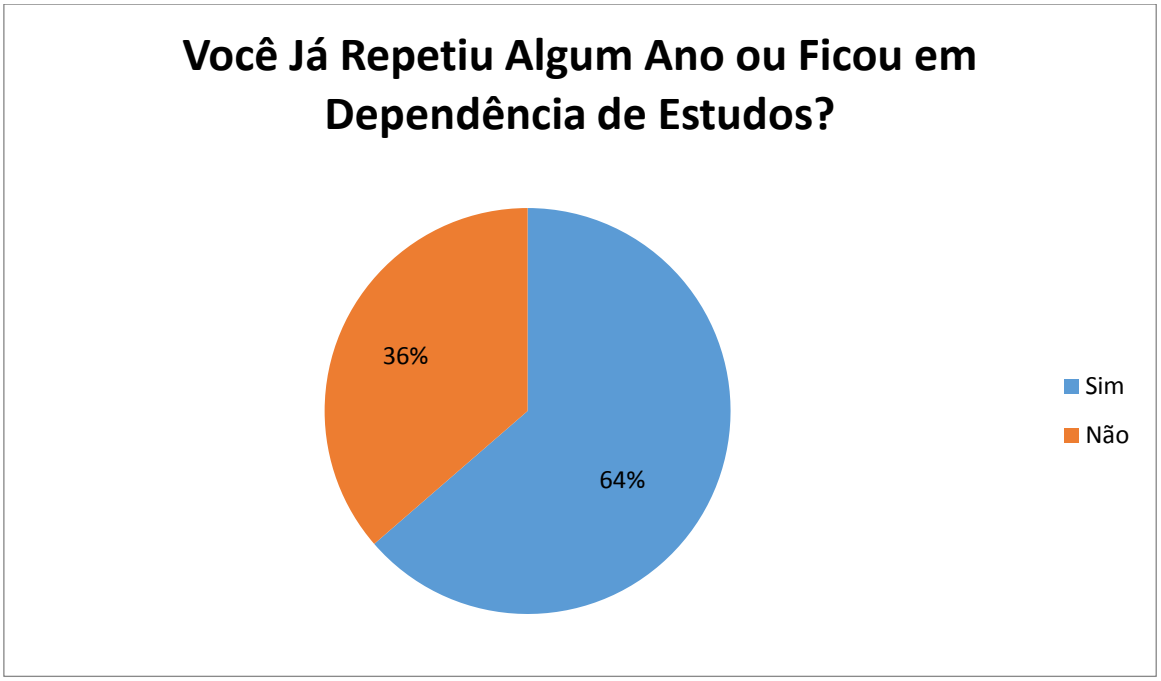


Gráfico 4: "Você Já Repetiu de Ano ou Ficou em Dependência de Estudos?"
Fonte: Do Autor

Por último, dos dados do questionário pré-atividades, gostaríamos de apresentar, no Gráfico 5: "Você Já Ouviu Falar em Criptografia?", os resultados para a pergunta: você já ouviu falar em Criptografia?

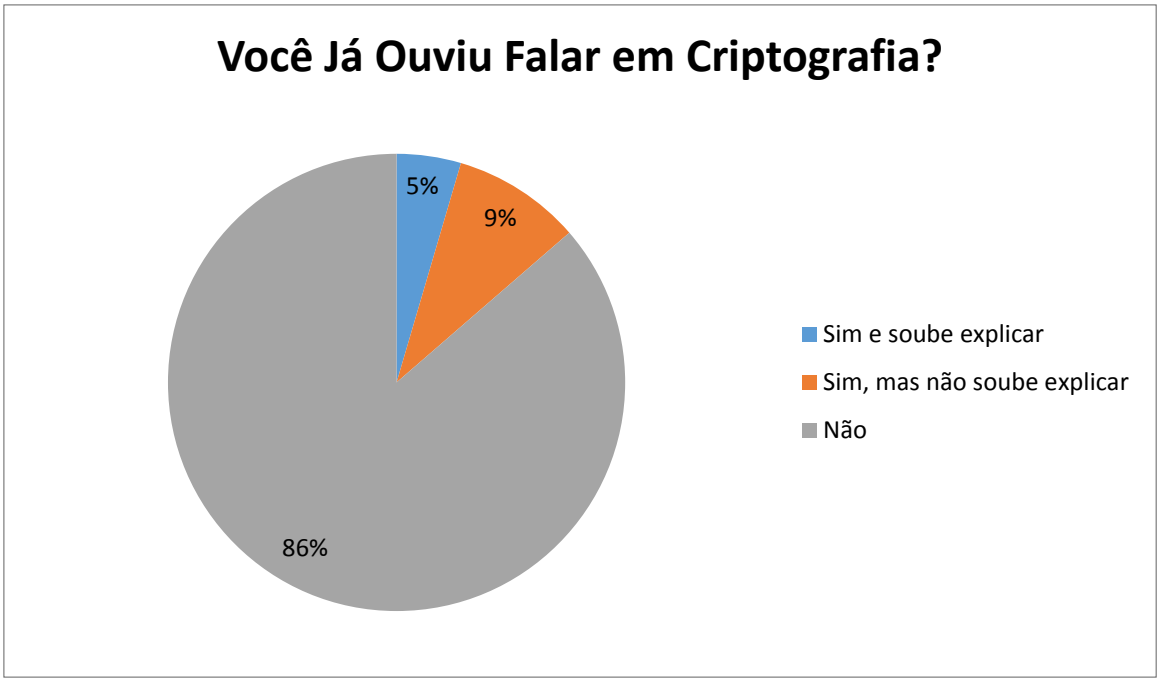
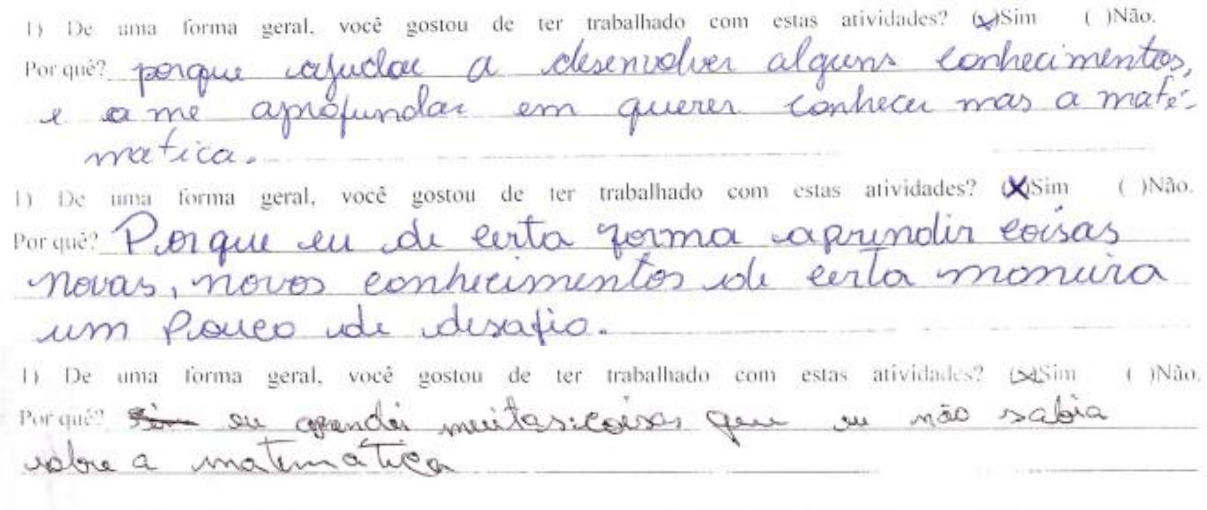


Gráfico 5: "Você Já Ouviu Falar em Criptografia?"
Fonte: Do Autor

Após a fase de Experimentação foi aplicado o questionário pós-atividades, com o intuito apenas de auxiliar a análise dos resultados obtidos com a sequência didática. Alguns dos resultados obtidos com este questionário achamos importante comentar aqui.

A primeira pergunta feita no questionário foi: Você gostou de ter trabalhado com estas atividades? Por quê? Os alunos foram unânimes ao dizer que sim, haviam gostado de trabalhar com a sequência didática proposta. Todos eles deram explicações do porquê de terem gostado, fato que nos deixou bastante satisfeitos com a aceitação do trabalho. Veja algumas das respostas dos alunos (Figura 47: Respostas Dadas para o Item 1 do Questionário Pós-Atividades).


1) De uma forma geral, você gostou de ter trabalhado com estas atividades? (X)Sim ( )Não.
Por quê? porque ajudou a desenvolver alguns conhecimentos, e a me aprofundar em querer conhecer mas a matemática.

1) De uma forma geral, você gostou de ter trabalhado com estas atividades? (X)Sim ( )Não.
Por quê? Porque eu de certa forma aprendir coisas novas, novos conhecimentos de certa maneira um pouco de desafio.

1) De uma forma geral, você gostou de ter trabalhado com estas atividades? (X)Sim ( )Não.
Por quê? ~~Sim~~ eu aprendi muitas coisas que eu não sabia sobre a matemática

Figura 47: Respostas Dadas para o Item 1 do Questionário Pós-Atividades
Fonte: Do Autor

A segunta pergunta foi: Agora você saberia dizer o que é Criptografia? Novamente todos os alunos responderam esta pergunta, de formas bastante variadas, mas dentro de um bom nível de aceitação, este fato também nos deixou bastante animados. Acompanhe algumas das respostas dadas pelos alunos (Figura 48: Respostas Dadas para o Item 2 do Questionário Pós-Atividades).

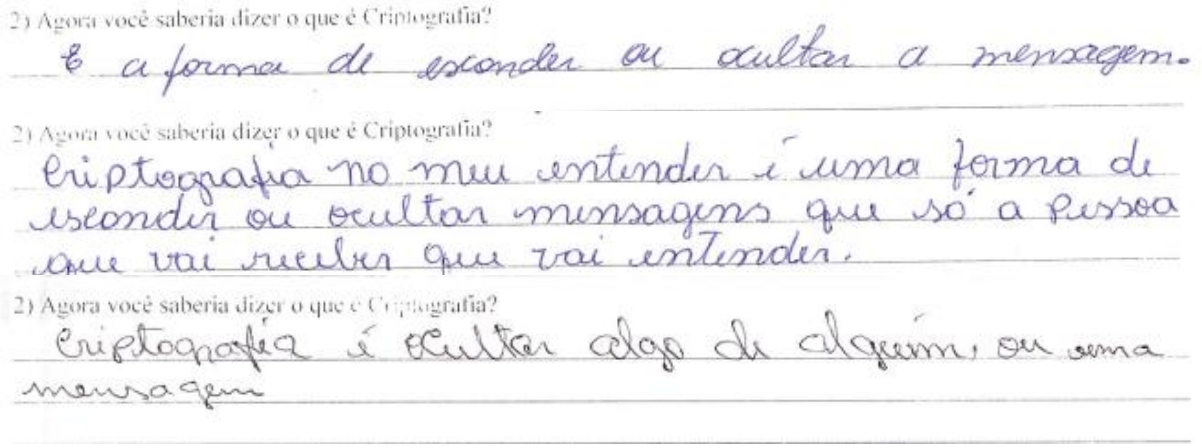


Figura 48: Respostas Dadas para o Item 2 do Questionário Pós-Atividades
Fonte: Do Autor

Em um dos itens do questionário, pedimos aos alunos que dessem uma nota de 1 a 5 para a experiência com este trabalho, os resultados estão apresentados no Gráfico 6:"Nota dada à Experiência".

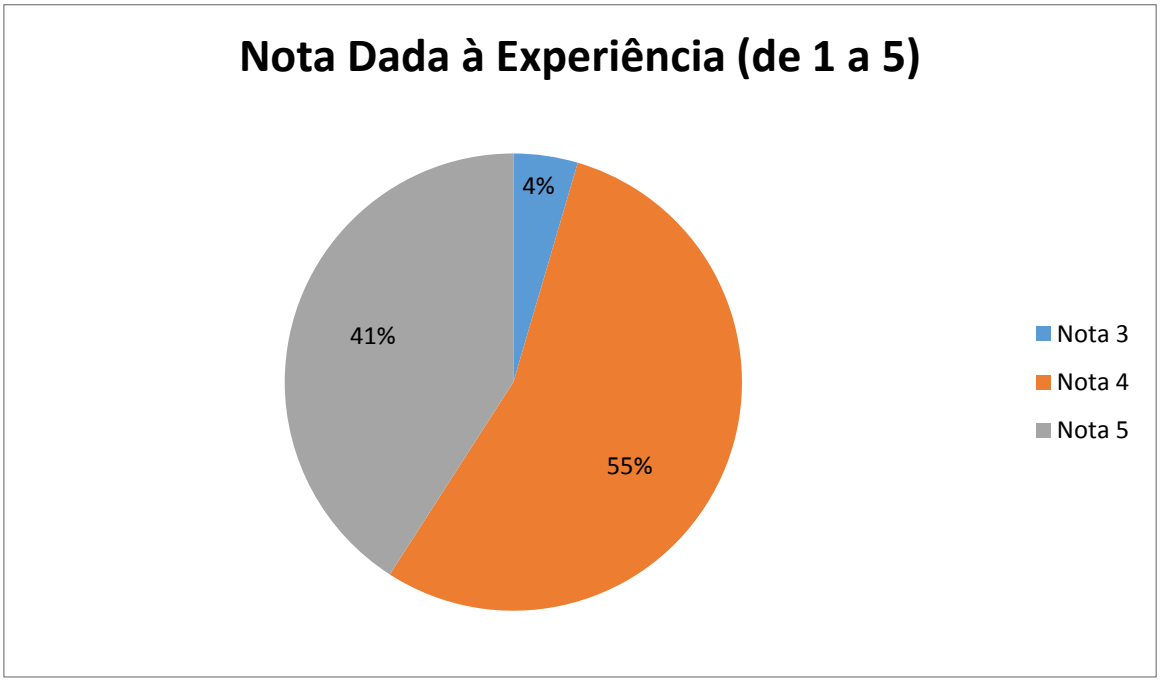


Gráfico 6:"Nota dada à Experiência"
Fonte: Do Autor

Outra pergunta feita no questionário foi: Você gostaria de trabalhar outros assuntos (conteúdos) de Matemática de forma semelhante? Os alunos foram unânimes ao dizer que

sim. Isto revela como é importante que sejam trabalhados alguns conteúdos, não só de Matemática, de forma contextualizada (aplicada).

Em um dos itens do questionário, foi solicitado aos alunos que dessem nota de 1 a 5 para o grau de dificuldade encontrado na resolução das atividades ou na compreensão dos conteúdos relacionados (sendo 1: "Pouca ou nenhuma dificuldade"; e 5: "Dificuldade extrema"). As respostas dadas pelos alunos estão apresentadas no Gráfico 7: "Dificuldades Encontradas nas Atividades ou Conteúdos".

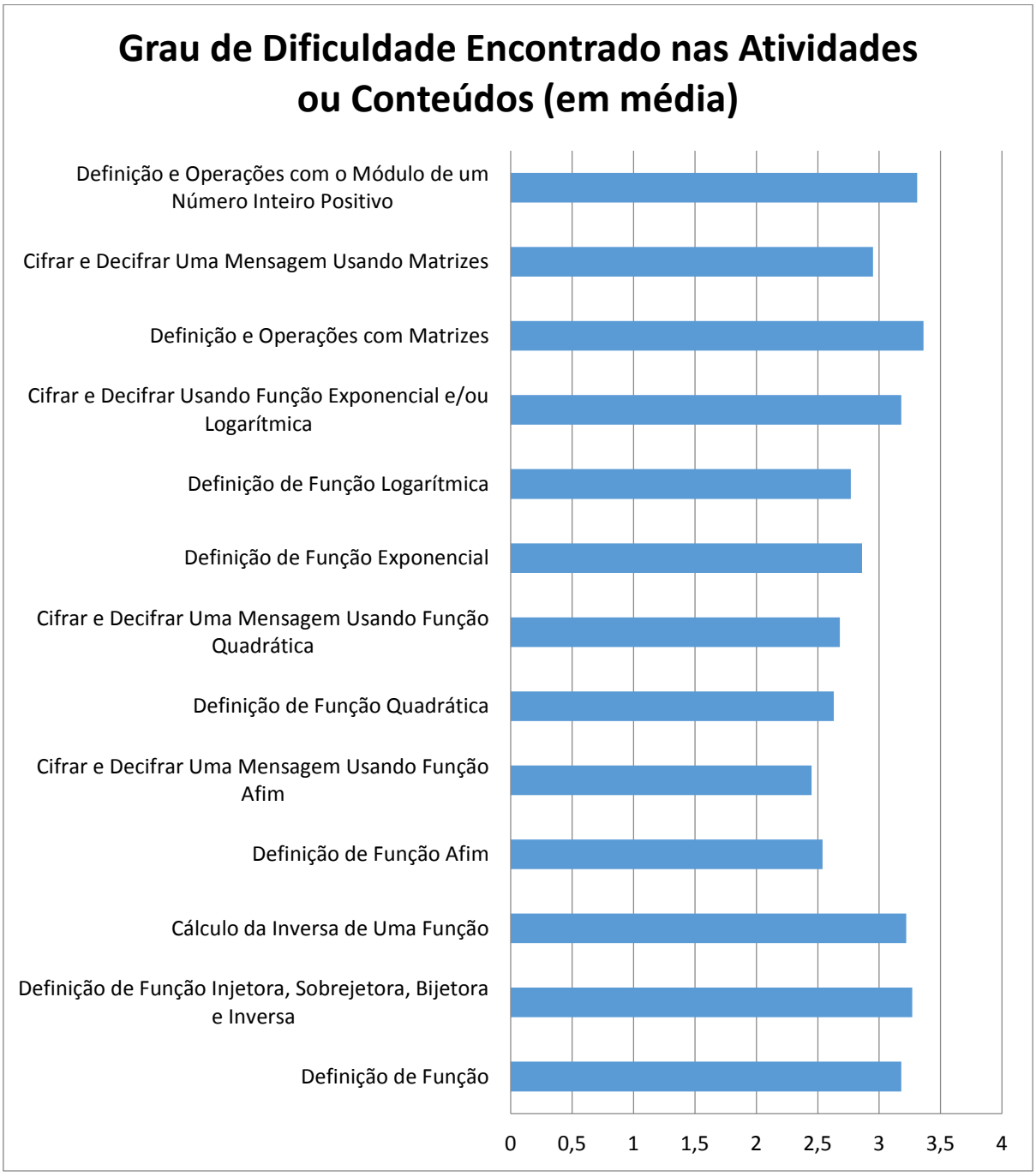


Gráfico 7: "Dificuldades Encontradas nas Atividades ou Conteúdos"
Fonte: Do Autor

No último item do questionário pós-atividades pedimos aos alunos que apontassem os pontos positivos e negativos das atividades desenvolvidas e de que forma eles acreditavam que poderíamos melhorar esta experiência. Veja abaixo algumas das respostas dadas pelos alunos (Figura 49: Respostas Dadas para o Item 8 do Questionário Pós-Atividades).

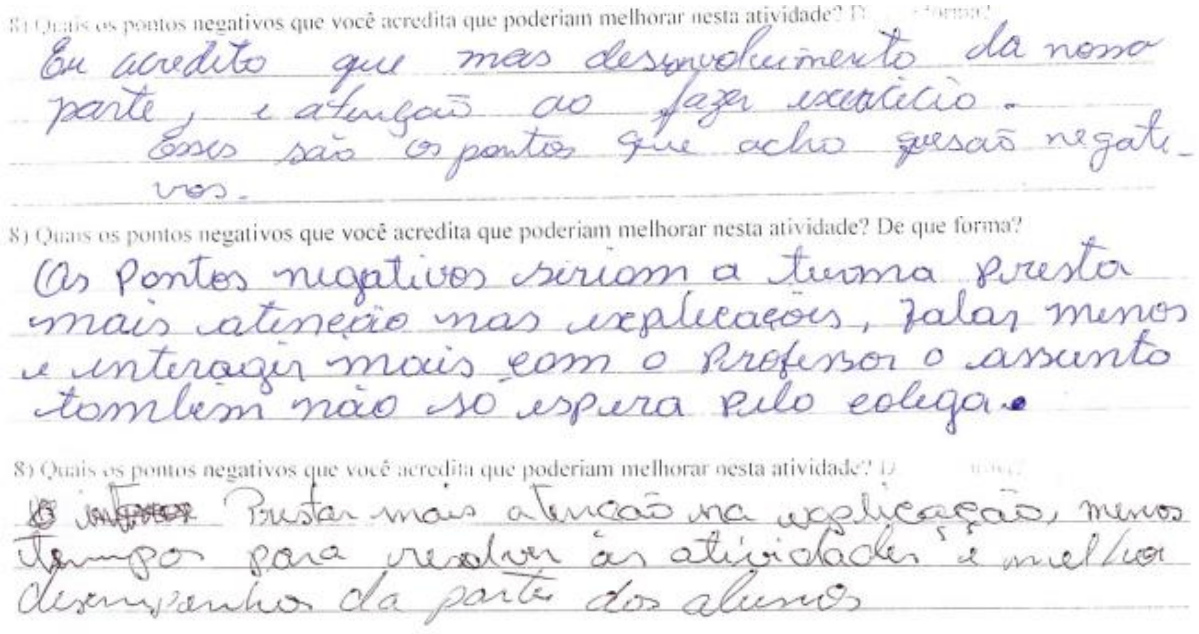


Figura 49: Respostas Dadas para o Item 8 do Questionário Pós-Atividades
Fonte: Do Autor

A grande maioria dos alunos citou questões centradas no próprio comportamento deles, como aumentar o poder de concentração nas explicações do professor e na resolução das atividades para poupar tempo. Isto se explica pelo fato de que alguns alunos terminavam a atividade rapidamente e, tinham que ficar esperando os outros colegas, que em algumas ocasiões, se atrasavam por ficarem conversando demais entre eles.

CONCLUSÃO

Observou-se, neste trabalho, que uma sequência didática com o tema Criptografia possibilitou aos alunos associar os conteúdos matemáticos trabalhados, às vezes de forma enfadonha, no ensino médio (funções e matrizes) a um tema atual e de relevância para o cotidiano deles (a codificação e decodificação de mensagens secretas). Possibilitou ainda revisar conteúdos que já haviam sido esquecidos, além de obter o conhecimento de conteúdos novos como tópicos de Aritmética Modular, a obtenção da inversa de uma Função Quadrática e cálculo da inversa módulo 26 de uma matriz quadrada $\boldsymbol{A}$ de ordem 2.

A aplicação da sequência didática permitiu ainda uma maior interação entre os alunos, além de promover o trabalho em grupo e a divisão de tarefas para a realização de um objetivo. Também possibilitou desenvolver as capacidades de concentração nas atividades e desenvolvimento de estratégias para resolução de problemas.

Devemos salientar que atividades envolvendo o tema Criptografia abrem caminho para a introdução, em sala de aula, de tecnologias da informação e comunicação. No nosso caso utilizamos a calculadora, mas este tema abre um grande leque de possibilidades para a utilização de softwares e outras tecnologias. A aplicação da sequência didática permitiu aos alunos explorar vários recursos da calculadora científica, facilitando cálculos longos e, em consequência, reduzindo o tempo de resolução das atividades.

A utilização da Engenharia Didática, como metodologia da pesquisa, possibilitou que a análise dos dados fosse feita internamente, validando as atividades desenvolvidas. Nesse contexto, a Engenharia Didática, consolida-se como um importante instrumento para o aperfeiçoamento do professor em sala de aula, ao permitir uma profunda análise do cotidiano da sala de aula.

Vale ressaltar que as hipóteses levantadas neste trabalho foram validadas através da sequência didática proposta para o segundo ano do Ensino Médio e, também, através das análises feitas na fase de análise a posteriori e validação. Durante a análise a posteriori e validação, verificou-se que os objetivos traçados nas fases anteriores foram alcançados, em sua maioria, pois os alunos conseguiram realizar as correlações entre os conteúdos do ensino médio e o tema abordado e conseguiram resolver problemas que necessitavam de conhecimentos específicos de conteúdos de matemática do Ensino Médio. Além disso, ao analisarmos os questionários pré e pós atividades, verificamos que, antes da experiência, apenas um aluno sabia o que era Criptografia e, após, todos souberam responder o que é Criptografia.

A sequência didática desenvolvida e aplicada neste trabalho pode ser entendida como um exemplo de material didático, que pode ser utilizado por professores em sala de aula, para fixar e revisar conteúdos matemáticos do ensino médio. Além de ser um bom motivador para despertar a curiosidade nos alunos e aumentar a afinidade dos alunos com a Matemática.

Acreditamos que temas como este, que permitem o desenvolvimento de atividades didáticas em sala de aula, devem ser abordados com maior frequência pelos professores, pois o currículo de matemática do Ensino Médio precisa ser estimulante, inovador e motivador para o aluno. Sabemos, no entanto, que alguns conteúdos de matemática do Ensino Médio têm uma maior dificuldade de serem aplicados ao cotidiano dos alunos. Isto posto, deve-se trabalhar, na medida do possível, os conteúdos que permitem aplicações, de forma didática e instigante. Vale citar que na análise dos questionários aplicados aos alunos, apenas um aluno destacou a Matemática como sua disciplina favorita. Deve-se buscar reverter esta situação de preterimento da Matemática, tornando-a o mais atrativa possível.

REFERÊNCIAS

ALENCAR, J. P. D. **Aritmética Modular e Criptografia**. profmat-sbm, 2013. Disponível em: <http://bit.profmat-sbm.org.br/xmlui/handle/123456789/912>. Acesso em: 24 Agosto 2015.

ALMOULOUD, S. A.; COUTINHO, C. D. Q. E. S. **Engenharia Didática: características e seus usos em trabalhos apresentados no GT-19/ANPEd**. periodicos.ufsc.br, 2008. Disponível em: <periodicos.ufsc.br/index.php/revemat/article/download/1981-1322.2008v3n1p62/12137+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 04 setembro 2015.

ALMOULOUD, S. A.; SILVA, M. J. F. **Engenharia Didática: Evolução e Diversidade**. periodicos.ufsc.br, 2012. Disponível em: <https://periodicos.ufsc.br/index.php/revemat/article/viewFile/1981-1322.2012v7n2p22/23452+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 12 Setembro 2015.

ALMOULOUD, S. A.; SILVA, M. J. F. D. **Engenharia Didática: evolução e diversidade**. periodicos.ufsc.br, 2012. Disponível em: <periodicos.ufsc.br/index.php/revemat/article/viewFile/1981-1322.2012v7n2p22/23452+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 06 setembro 2015.

ANTON, H.; RORRES, C. **Álgebra Linear com Aplicações**. 8ª. ed. Porto Alegre: Bookman, 2001. 466-473 p.

BERENGUER, M. I. S. **A Aplicação da Engenharia Didática no Ensino das Ciências Exatas**. avm.edu.br, 2010. Disponível em: <http://www.avm.edu.br/docpdf/monografias_publicadas/t205982.pdf>. Acesso em: 16 Setembro 2015.

BRASIL. **Parâmetros Currículares Nacionais: Ensino Médio - Parte III - Ciências da Natureza, Matemática e Técnologias**. portal mec, 2000. Disponível em: <portal.mec.gov.br/seb/arquivos/pdf/blegais.pdf>. Acesso em: 14 Agosto 2015.

BRASIL. **Lei de Diretrizes e Bases da Educação Nacional, Lei 9394 de 20 de Dezembro de 1996**. Câmara dos Deputados, 2015. Disponível em: <www2.camara.leg.br/legin/fed/lei/1996/lei-9394-20-dezembro-1996-362578-norma-pl.html+&cd=4&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 14 Agosto 2015.

BRUM, W. P. **Contribuições da Engenharia Didática no Ensino de Matemática: Análise e Reflexão de uma Experiência Didática para o Estudo de geometria Esférica**. sinect.com.br, 2013. Disponível em: <http://sinect.com.br/anais2014/anais2014/artigos/ensino-de-matematica/01403926013.pdf+&cd=10&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 17 Setembro 2015.

CARNEIRO, V. C. G. **Engenharia Didática: Um Referencial Para Ação Investigativa e Para a Formação de Professores de Matemática**. www.ufrgs.br, 2005. Disponível em: <www.ufrgs.br/espmat/disciplinas/midias_digitais_II_2014/modulo_III/ENGENHARIA_ZETEIKE2005.pdf>. Acesso em: 12 Julho 2015.

CERVO, A. L.; BERVIAN, P. A.; DA SILVA, R. **Metodologia Científica**. 6a. ed. São Paulo: Pearson Prentice Hall, 2007.

COSTA, D. D. **A Matemática e os Códigos Secretos: Uma Introdução à Criptografia**. profmat-sbm, 2014. Disponível em: <bit.profmat-sbm.org.br/xmlui/handle/123456789/1080>. Acesso em: 23 agosto 2015.

COUTINHO, S. C. **Apostila 7: Criptografia**. Obmep - PIC, 2009. Disponível em: <http://www.obmep.org.br/docs/apostila7.pdf>. Acesso em: 13 Junho 2015.

DAINEZE, K. C. S. A. D. L. **Números Primos e Criptografia: Da Relação com a Educação ao Sistema RSA**. profmat-sbm, 2013. Disponível em: <bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/518/2011_00416_KELLY_CRISTINA_SANTOS_ALEXANDRE_DE_LIMA.pdf%3Fsequence%3D1+&cd=2&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 10 junho 2015.

DOLCE, O.; IEZZI, G.; MURAKAMI, C. **Fundamentos de Matemática Elementar**. 10ª Edição. ed. São Paulo: Atual, v. 2, 2013.

FIARRESGA, V. M. C. **Criptografia e Matemática**. repositorio.ul, 2010. Disponível em: <repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf+&cd=3&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 06 junho 2015.

FREIRE, P. B.; CASTILHO, J. E. **A Matemática dos Códigos Criptográficos**. ucb, 2007. Disponível em: <www.ucb.br/sites/100/103/TCC/12007/PalomaBarbosaFreire.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 18 junho 2015.

GIL, A. C. Como Classificar as Pesquisa? In: GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 5a. ed. São Paulo: Ed. Atlas S.A., 2010. Cap. 4, p. 25-26.

GOMES, F. C. L. **Uma Proposta de Abordagem no Ensino Médio da Criptografia RSA e sua Estrutura Matemática**. profmat-sbm, 2014. Disponível em: <bit.profmat-sbm.org.br/xmlui/handle/123456789/1365>. Acesso em: 21 agosto 2015.

GOMEZ, H. C. M. **Reflexões Sobre uma Prática de Ensino: Uma Engenharia Didática**. mat.ufrgs.br, 2008. Disponível em: <www.mat.ufrgs.br/~vclotilde/orientacoes/tcc.pdf/Microsoft%2520Word%2520-%2520TCC_Helena_Carina_Malaguez_Gomes_144112.pdf+&cd=3&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 18 Setembro 2015.

GROENWALD, C. L. O.; FRANKE, R. F. **Currículo de Matemática e o Tema Criptografia no Ensino Médio**. Educção Matemática em Revista, Porto Alegre - RS, 2008. 51-57.

GROENWALD, C. L. O.; OLGIN, C. A. **Currículo de Matemática no Ensino Médio: Atividades Didáticas com o tema Criptografia**. www.gente.eti.br, 2011. Disponível em: <www.gente.eti.br/lematec/CDS/XIIICIAEM/artigos/691.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 14 julho 2015.

GROENWALD, C. L. O.; OLGIN, C. D. A. **Códigos e Senhas: Sequência Didática com o Tema Criptografia no Ensino Fundamental**. lematec, 2010. Disponível em: <www.lematec.net/CDS/ENEM10/artigos/CC/T17_CC555.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 12 Agosto 2015.

HAZZAN, S.; IEZZI, G. **Fundamentos de Matemática Elementar**. 8ª Edição. ed. São Paulo: Atual, v. 4, 2012.

HEFEZ, A. **Iniciação à Aritmética**. obmep.org.br, 2009. Disponível em: <www.obmep.org.br/export/sites/default/arquivos/apostilas_pic2010/Apostila1-aritmetica.pdf+&cd=10&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 20 Julho 2015.

HEFEZ, A. **Elementos de Aritmética**. 2ª Edição. ed. Rio de Janeiro: SBM, 2011.

IEZZI, G.; MURAKAMI, C. **Fundamentos de Matemática Elementar**. 9ª Edição. ed. São Paulo: Atual, v. 1, 2013.

JESUS, A. L. N. D. **Criptografia na Educação Básica**. profmat-sbm, 2013. Disponível em: <bit.profmat-sbm.org.br/xmlui/handle/123456789/872>. Acesso em: 24 agosto 2015.

JUNIOR, S. D. S. C. **Criptografia via Curvas Elípticas**. profmat-sbm, 2013. Disponível em: <bir.profmat-sbm.org.br/xmlui/handle/123456789/853>. Acesso em: 23 agosto 2015.

LIMA, E. L. et al. **A Matemática do Ensino Médio**. 9ª Edição. ed. Rio de Janeiro: SBM, v. 1, 2006.

LIMA, E. L. et al. **A Matemática do Ensino Médio**. 6ª Edição. ed. Rio de Janeiro: SBM, v. 2, 2006.

LOUREIRO, F. O. **Tópicos de Criptografia para o Ensino Médio**. profmat-sbm, 2014. Disponível em: <bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/1528/2012_01339_FLAVIO_ORNELLAS_LOUREIRO.pdf%3Fsequence%3D1+&cd=2&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 05 julho 2015.

MARQUES, T. V. **Criptografia: Abordagem Histórica, Protocolo Diffie-Hellman e Aplicações em Sala de Aula**. profmat-sbm, 2013. Disponível em: <http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/281/2011_00133_THIAGO_VALENTIM_MARQUES.pdf?sequence=1>. Acesso em: 20 junho 2015.

NETO, L. A. D. S. **Aritmética Modular e Criptografia no Ensino Básico**. profmat-sbm, 2014. Disponível em: <bit.profmat-sbm.org.br/xmlui/handle/123456789/1502>. Acesso em: 22 agosto 2015.

OLGIN, C. D. A. **Currículo no Ensino Médio: Uma Experiência com o Tema Criptografia**. www.ppgecim.ulbra.br, 2011. Disponível em: <www.ppgecim.ulbra.br/teses/index.php/ppgecim/article/view/138+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 21 junho 2015.

OLGIN, C. D. A.; GROENWALD, C. L. O.; FRANKE, R. F. **Criptografia no Ensino Médio**. Sbembrasil, 2011. Disponível em: <www.sbembrasil.org.br/files/ix_enem/Poster/Trabalhos/PO88388417053T.doc+&cd=5&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 11 Junho 2015.

OLIVEIRA, M. M. D. **Sequência Didática Interativa no Processo de Formação de Professores**. www.pasem.org, 2013. Disponível em: <http://www.pasem.org/gestion/archivos/experiencias/25/SDI-Texto%20Completo%20do%20Livro.pdf>. Acesso em: 21 Julho 2015.

PANTOJA; SILVA, L. F. L. F. H. S. **Engenharia Didática: Articulando Um Referencial Metodológico Para o Ensino de Matemática na EJA**. www.sbembrasil.org.br, 2012. Disponível em: <www.sbembrasil.org.br/files/ix_enem/Comunicacao_Cientifica/Trabalhos/CC63265869253T.doc>. Acesso em: 22 Julho 2015.

PIVATTO, W.; SCHUHMACHER, E. **As Contribuições da Engenharia Didática Enquanto Campo Metodológico Para o Ensino de Geometria Esférica**. publicacoes.unigranrio.edu.br, 2013. Disponível em:

<publicacoes.unigranrio.edu.br/index.php/recm/article/view/2071/1107+&cd=9&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 17 Setembro 2015.

POMMER, W. M. **A Engenharia Didática em Sala de Aula: Elementos Básicos e Uma Ilustração Envolvendo as Equações Diofantinas Lineares**. stoa.usp.br, 2013. Disponível em: <http://stoa.usp.br/wmpommer/files/3915/20692/Livro%2BEng%25C2%25AA%2BDid%25C3%25A1tica%2B2013.pdf>. Acesso em: 23 Julho 2015.

QUARESMA, P. **Criptografia**. www.mat.uc.pt, 2008. Disponível em: <http://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia1011/artigo-gazeta08.pdf>. Acesso em: 15 Junho 2015.

RIBEIRO, D. F.; LOURENÇANO, P. G. P.; COSTA, A. D. D. **Criptografia: Uma Aplicação da Matemática Discreta Através da Implementação da Cifra de César em VISUALOG**. fatectq, 2013. Disponível em: <http://www.fatectq.edu.br/interfacetecnologica/arquivos/volume10/artigo02.pdf>. Acesso em: 04 julho 2015.

SANTOS, J. L. D. **A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Mtemática Básica**. profmat-sbm, 2013. Disponível em: <bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/208/2011_00046_JOSE_LUIZ_DOS_SANTOS.pdf%3Fsequence%3D1+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 22 junho 2015.

SANTOS, J. P. D. O. **Introdução à Teoria dos Números**. 3ª. ed. Rio de Janeiro: IMPA, 2014.

SCHURMANN, H. A. **Criptografia Matricial aplicada ao Ensino Médio**. profmat-sbm, 2013. Disponível em: <bit.profmat-sbm.org.br/xmlui/handle/123456789/916>. Acesso em: 24 agosto 2015.

SIDKI, S. **Introdução à Teoria dos Números**. impa.br, 2009. Disponível em: <www.impa.br/opencms/pt/biblioteca/cbm/10CBM/10_CBM_75_09.pdf+&cd=8&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 12 Julho 2015.

SOUZA, C. A. D. **Influências da Engenharia Didática Francesa na Educação Matemática no Brasil: a circulação e a apropriação de ideias**. cibem7.semur.edu, 2013. Disponível em: <www.cibem7.semur.edu.uy/7/actas/pdfs/346.pdf+&cd=2&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 05 Setembro 2014.

SOUZA, R. N. S. D.; CORDEIRO, M. H. **A Contribuição da Engenharia Didática para a Prática Docente de Matemática na Educação Básica**. pucpr.br, 2005. Disponível em:

<www.pucpr.br/eventos/educere/educere2005/anaisEvento/documentos/painel/TCCI200.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 06 setembro 2015.

TAMAROZZI, A. C. **Codificando e Decifrando Mensagens**. Revista do Professor de Matemática - RPM, São Paulo, v. 45, 2001.

TERADA, R. **Criptografia e a Importância das Suas Aplicações**. RPM, São Paulo, v. 12, 1988.

ZATTI, S. B.; BELTRAME, A. M. **A Presença da Álgebra Linear e Teoria dos Números na Criptografia**. unifra - jornal da educção, 2006. Disponível em: <www.unifra.br/eventos/jornadaeducacao2006/2006/pdf/artigos/matem%25C3%25A1tica/A%2520PRESEN%25C3%2583A%2520DA%2520-LGEBRA%2520LINEAR%2520E%2520TEORIA%2520DOS%2520N%2BMEROS%2520NA%2520CRIPT%25C3%25A0.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 02 julho 2015.

APÊNDICE A – Questionário Pré-Atividades

1) Qual a sua idade?_____

2) Qual a sua disciplina favorita?_____

3) Você exerce atividade remunerada além de estudar? ( )Sim ( )Não

4) Caso você trabalhe, quantas horas por dia você dedica a essa atividade?_____

5) Você já repetiu algum ano de estudo ou ficou em dependência de estudos? ( )Sim ( )Não

6) Se sua resposta for sim, qual o ano ou qual a disciplina (no caso de dependência)? Ano:_____ Disciplina:_____

7) Você acha que a matemática é fundamental no seu dia a dia? ( )Sim ( )Não. Por quê?_____

_____

_____

8) Você já usou matemática para resolver algum problema do seu dia a dia? ( )Sim ( )Não. De que forma?_____

_____

_____

9) Você estuda em casa além do que os seus professores passam em sala de aula? ( )Sim ( )Não

10) Caso você tenha respondido sim, quantas vezes por semana e quantas horas você dedica para os estudos em casa?_____

11) Você se sente estimulado a pesquisar mais e estudar matemática em casa? ( )Sim ( )Não. Por quê?_____

_____

_____

12) Como as aulas de matemática são ministradas? Você pode marcar mais de uma opção, caso ache necessário

( ) Aulas expositivas (usando quadro e marcador);

( ) Aulas expositivas utilizando material impresso (apostilas e/ou livro);

( ) Aulas expositivas utilizando recursos multimídias (computador, softwares, projetor, etc);

( ) Aulas interativas com atividades em grupos;

( ) Aulas teóricas associadas a aplicações dentro ou fora de sala;

( ) Alguma outra não mencionada;

13) Você possui smartphone ou calculadora científica? ( )Sim ( )Não. Alguma vez você usou calculadora científica? ( )Sim ( )Não.

14) Você já ouviu falar em Criptografia? Saberia dizer o que é?

APÊNDICE B – Questionário Pós-Atividades

1) De uma forma geral, você gostou de ter trabalhado com estas atividades? ( )Sim ( )Não. Por quê?_____

_____

_____

2) Agora você saberia dizer o que é Criptografia?_____

_____

_____

3) Você acha que aprendeu alguma coisa com essas atividades? ( )Sim ( )Não. O quê?_____

_____

_____

4) De 1 a 5, que nota você daria para essa experiência?_____

5) Você gostaria de trabalhar outros assuntos da matemática de forma semelhante? ( )Sim ( )Não.

6) O uso da calculadora ajudou na resolução das atividades? ( )Sim ( )Não. De que forma?_____

_____

_____

7) Sobre o grau de dificuldade encontrado na resolução das atividades ou na compreensão dos conteúdos relacionados, sendo 1: "pouca ou nenhuma dificuldade"; e 5: "extremamente difícil". Dê nota de 1 a 5 para os itens:

Definição de Função: ( )

Definição de Função Injetora, Sobrejetora, Bijetora e Inversa: ( )

Cálculo da inversa de uma Função: ( )

Definição de Função Afim: ( )

Criptografar e desincriptar uma mensagem usando Função Afim: ( )

Definição de Função Quadrática: ( )

Criptografar e desincriptar uma mensagem usando Função Quadrática: ( )

Definição de Função Exponencial: ( )

Definição de Função Logarítmica: ( )

Criptografar e desincriptar uma mensagem usando Função Exponencial e/ou Logarítmica: ( )

Definição e operações com Matrizes: ( )

Criptografar e desincriptar uma mensagem usando Matrizes: ( )

Definição e operações com o módulo de um número inteiro positivo: ( )

8) Quais os pontos negativos que você acredita que poderiam melhorar nesta atividade? De que forma?

APÊNDICE C – Material Impresso Dado aos Alunos

Atividade 1:

Inicialmente, iremos relacionar números ao nosso alfabeto (o símbolo # representa um espaço em branco), com o auxílio da tabela abaixo:

#	A	B	C	D	...	V	W	X	Y	Z
0	1	2	3	4	...	22	23	24	25	26

Portanto, cifrar uma mensagem recai no problema de permutar números por meio de uma regra *f*. Dessa forma, suponhamos que um casal apaixonado deseja trocar mensagens secretas, utilizando a tabela dada. Vamos ajudá-los a realizar tal intento, o primeiro passo a se tomar é definir a função cifradora, digamos $f(x) = 3x - 5$. Assim, por exemplo, à mensagem "AMO VOCÊ" associamos a sequência numérica 1 – 13 – 15 – 0 – 22 – 15 – 3 – 5, mas transmitimos a sequência: (-2) – 34 – 40 – (-5) – 61 – 40 – 4 – 10. Observe que não são usados sinais de pontuação e/ou acentuação gráfica.

a) Paulo deseja enviar a mensagem "VAMOS NOS ENCONTRAR". Qual seria a sequência numérica criptografada para essa mensagem?

b) Ao receber a mensagem, qual deve ser o passo a passo de Ana para ler (decodificar) a mensagem? Qual o conceito matemático associado ao processo de decodificar uma mensagem nos moldes dado?

c) Paulo recebe a sequência numérica: 55 – 10 – (-5) –10 – 37 – 4 – 40 – 37 – 55 – 49 – 40 – (-5) – (-2) – 43 – 40 – 52 – (-5) – (-2) – (-5) – (-2) – 58 – 31 – (-2). Qual a mensagem decodificada recebida por Paulo?

d) Um "espião" apoderou-se de um pedaço de papel no qual havia uma correspondência entre dois pares de números da sequência numérica decodificada por Paulo (item anterior) e ele sabe que a função codificadora é afim, seria ele capaz de ler qualquer outra mensagem trocada pelo casal? Em caso afirmativo, explique como isso seria feito?

e) Crie uma mensagem curta, codifique-a usando uma função afim de sua preferência e, envie-a para um grupo de sua escolha, indicando em sua mensagem qual foi a sua função escolhida.

f) Decodifique a mensagem recebida pelo seu grupo.

Atividade 2: Com base na tabela dada na atividade 5.1 e usando a função cifradora $f(x) = x^2 - 4x + 4$, faça o que se pede:

a) Cifre a mensagem "AMO A MATEMÁTICA";

b) Você recebeu a mensagem codificada: 9 – 289 – 324 – 361 – 4 – 9 – 1 – 169 – 121 – 1 – 16 – 49 – 144 – 1 – 169. Decodifique a mensagem (observe que serão necessárias algumas tentativas para as imagens inversas repetidas);

c) Quais os conceitos matemáticos envolvidos na resolução do item "b"?

d) A função cifradora $f(x) = x^2 - 4x + 4$ usada foi uma boa escolha? Por quê?

e) Como você faria para corrigir o problema das imagens inversas repetidas?

f) Crie uma mensagem curta, em seguida, usando uma função quadrática de sua escolha codifique-a e a envie para um grupo de sua preferência, não se esqueça de informar a função cifradora escolhida para que o outro grupo seja capaz de decifrar a mensagem.

g) Decodifique a mensagem recebida pelo seu grupo.

Atividade 3: Ainda com base na tabela dada na atividade 4.1, mas agora utilizando a função cifradora $f(x)=2^x$, faça o que se pede:

a) Codifique a mensagem "CRIPTOGRAFAR É DIVERTIDO", usando a função dada no enunciado;

b) Você recebeu a mensagem codificada: 2 – 8192 – 32 – 2 – 8192 – 2 – 1048576 – 32 – 8192 – 2 – 1048576 – 512 – 8 – 2, que foi obtida ao se utilizar a função cifradora dada no enunciado. Decodifique-a;

c) Quais os conceitos matemáticos envolvidos nos dois itens anteriores?

d) Crie uma mensagem curta, codifique-a usando a função logarítmica $y=\log_{10} x$ e a envie para um grupo de sua preferência;

e) Decodifique a mensagem recebida pelo seu grupo;

Atividade 4: Após terem suas mensagens decodificadas por um "espião", suponhamos agora que Ana e Paulo combinem de utilizar as matrizes $A=\begin{pmatrix}1 & 2\\ 2 & 3\end{pmatrix}$ e $A^{-1}=\begin{pmatrix}-3 & 2\\ 2 & -1\end{pmatrix}$ como chaves para codificar suas mensagens. Para transmitir a mensagem "TESTE DE CHAVE", Paulo inicialmente monta uma matriz mensagem M (usando a tabela dada na questão anterior) dispondo a sequência numérica associada à mensagem em colunas e completando a posição restante com o 0, obtendo:

$$M=\begin{pmatrix}20 & 19 & 5 & 4 & 3 & 1 & 5\\ 5 & 20 & 0 & 5 & 8 & 22 & 0\end{pmatrix}.$$

Feito isto, codificou a mensagem usando a matriz A, calculando:

$$AM=\begin{pmatrix}1 & 2\\ 2 & 3\end{pmatrix}\begin{pmatrix}20 & 19 & 5 & 4 & 3 & 1 & 5\\ 5 & 20 & 0 & 5 & 8 & 22 & 0\end{pmatrix}$$
$$=\begin{pmatrix}30 & 59 & 5 & 14 & 19 & 45 & 5\\ 55 & 98 & 10 & 23 & 30 & 68 & 10\end{pmatrix},$$

e transmite a sequência numérica: 30 – 55 – 59 – 98 – 5 – 10 – 14 – 23 – 19 – 30 – 45 – 68 – 5 – 10. Para decodificar (ler) a mensagem recebida, Ana, deve restaurar o formato da matriz AM, em seguida, com a chave decodificadora A^{-1} recupera a matriz M através da identidade matricial:

$$M=A^{-1}.(A.M)$$
$$M=\begin{pmatrix}-3 & 2\\ 2 & -1\end{pmatrix}.\begin{pmatrix}30 & 59 & 5 & 14 & 19 & 45 & 5\\ 55 & 98 & 10 & 23 & 30 & 68 & 10\end{pmatrix}$$
$$=\begin{pmatrix}20 & 19 & 5 & 4 & 3 & 1 & 5\\ 5 & 20 & 0 & 5 & 8 & 22 & 0\end{pmatrix}.$$

Observe que não são usados sinais de pontuação e/ou acentuação gráfica.

a) Ana quer enviar a mensagem "TE CURTO DE MONTÃO", qual deve ser a sequência numérica transmitida para Paulo?

b) Recebida a mensagem acima por Paulo, qual será o procedimento dele para poder ler

(decodificar) a mensagem? Qual o conceito matemático, associado ao processo de decodificar a mensagem, feito por Paulo?

c) Ana recebe a mensagem codificada: 33 – 52 – 33 – 51 – 52 – 85 – 47 – 79 – 33 – 51 – 26 – 46 – 43 – 70 – 15 – 29 – 34 – 53. Qual a mensagem original (após ser decodificada) enviada por Paulo?

d) Caso um "espião" venha a se apoderar da mensagem do item anterior e conhecendo a tabela da atividade 1, esses fatores seriam suficientes para decodificá-la? Em caso Negativo, o que mais o espião precisa para poder decodificar a mensagem interceptada?

e) Crie uma mensagem curta, usando uma matriz cifradora 2x2 (matriz *A*) de sua escolha; envie-a para outro grupo, não se esqueça de informar ao grupo escolhido a matriz A^{-1} que servirá para a decodificação de sua mensagem.

f) Decodifique a mensagem recebida pelo seu grupo.

Atividade 5: Primeiramente vamos associar cada letra do texto comum (claro) e do texto cifrado, excetuando-se o "Z", a um valor numérico que especifica sua posição no nosso alfabeto, dado pela tabela de associação abaixo

A	**B**	**C**	**D**	**...**	**V**	**W**	**X**	**Y**	**Z**
1	2	3	4	...	22	23	24	25	0

Por motivos que ficarão claros mais tarde, damos a "Z" o valor de 0.

Nos casos mais simples de cifras de Hill (nosso caso), transformamos pares sucessivos de texto comum em texto cifrado pelo seguinte procedimento:

1º Passo: Escolha uma matriz 2x2 $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ com entradas inteiras para efetuar a codificação. Condições adicionais sobre *A* serão impostas mais tarde.

2º Passo: Agrupe letras sucessivas do texto comum em pares, adicionando uma letra fictícia (no nosso caso repetiremos a última letra do texto claro) para completar o último par se o texto comum tiver um número ímpar de letras. Substitua cada letra do texto comum por seu equivalente numérico.

3º Passo: Converta cada par sucessivo p_1p_2 de letras do texto comum em um vetor coluna (matriz 2x1) $p=\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ e efetue o produto $\boldsymbol{Ap}$. Chamamos $\boldsymbol{p}$ de *vetor comum* e $\boldsymbol{Ap}$ o correspondente *vetor cifrado.*

4º Passo: Converta cada vetor cifrado em seu equivalente alfabético, usando a congruência (mod 26) e a tabela dada anteriormente.

Exemplo 1: Usando a matriz codificadora $A=\begin{pmatrix} 7 & 5 \\ 5 & 8 \end{pmatrix}$, desejamos codificar a mensagem: "CRIPTOGRAFIA" através da cifra de Hill.

Solução:

Vamos agrupar as letras do texto comum em pares, obtendo: CR – IP – TO – GR – AF – IA. Usando a tabela dada, encontramos a correspondência numérica: (3; 18) – (9; 16) – (20; 15) – (7; 18) – (1; 6) – (9; 1). Para codificar o par "CR", devemos efetuar o produto matricial $Ap=\begin{pmatrix} 7 & 5 \\ 5 & 8 \end{pmatrix}\cdot\begin{pmatrix} 3 \\ 18 \end{pmatrix}=\begin{pmatrix} 111 \\ 159 \end{pmatrix}$. Observe que os números 111 e 159 não possuem equivalente alfabético na tabela dada. Para resolver esse problema nós fazemos o seguinte acordo:

"Sempre que aparecer um inteiro maior que 25, ele será substituído pelo resto da divisão desse inteiro por 26". Como o resto da divisão por *26* é sempre um dos números *0, 1, 2, ..., 25*, este procedimento sempre fornece um inteiro com equivalente alfabético dado pela nossa tabela.

Assim, o vetor $\begin{pmatrix}111\\159\end{pmatrix}$ deve ser substituído por $\begin{pmatrix}7\\3\end{pmatrix}$, pois 7 é o resto da divisão de 111 por 26 e 3 é o resto da divisão de 159 por 26, e obtemos o par de letras cifradas "GC".

As contas para os outros vetores cifrados são:

$$\begin{pmatrix}7&5\\5&8\end{pmatrix}\cdot\begin{pmatrix}9\\16\end{pmatrix}=\begin{pmatrix}143\\173\end{pmatrix} ou \begin{pmatrix}13\\17\end{pmatrix}$$

$$\begin{pmatrix}7&5\\5&8\end{pmatrix}\cdot\begin{pmatrix}20\\15\end{pmatrix}=\begin{pmatrix}215\\220\end{pmatrix} ou \begin{pmatrix}7\\12\end{pmatrix}$$

$$\begin{pmatrix}7&5\\5&8\end{pmatrix}\cdot\begin{pmatrix}7\\18\end{pmatrix}=\begin{pmatrix}139\\179\end{pmatrix} ou \begin{pmatrix}9\\23\end{pmatrix}$$

$$\begin{pmatrix}7&5\\5&8\end{pmatrix}\cdot\begin{pmatrix}1\\6\end{pmatrix}=\begin{pmatrix}37\\53\end{pmatrix} ou \begin{pmatrix}11\\1\end{pmatrix}$$

$$\begin{pmatrix}7&5\\5&8\end{pmatrix}\cdot\begin{pmatrix}9\\1\end{pmatrix}=\begin{pmatrix}68\\53\end{pmatrix} ou \begin{pmatrix}16\\1\end{pmatrix}$$

Esses vetores correspondem, respectivamente, aos pares de textos cifrados "MQ", "GL", "IW", "KA", "PA". Juntando todos os pares de texto cifrados, obtemos a mensagem cifrada completa: GC – MQ – GL – IW – KA – PA, que seria transmitida como uma única cadeia de letras sem espaços: "GCMQGLIWKAPA".

Como o texto comum foi agrupado em pares e criptografado por uma matriz 2x2, dizemos que a cifra de Hill do nosso exemplo é uma *2-cifra de Hill*. Evidentemente também é possível agrupar o texto comum em ternos e criptografar com uma matriz 3x3 com entradas inteiras, esta cifra é chamada *3-cifra de Hill*. Em geral, para uma *n-cifra de Hill* agrupamos o texto comum em conjunto de *n* letras e criptografamos usando uma matriz *n* x *n* de entradas inteiras.

Aritmética Modular: No nosso exemplo substituímos os inteiros maiores do que 25 pelos seus respectivos restos pela divisão por 26. Esta técnica de trabalhar com os restos é a base de uma parte da Matemática chamada Aritmética Modular. Tendo em vista sua importância em criptografia, iremos fazer uma breve pausa para elaborar algumas das principais ideias desta área.

Congruência: Em Aritmética Modular nós supomos dado um inteiro positivo m, chamado módulo e consideramos "iguais" ou "equivalentes" (congruentes) em relação a esse módulo quaisquer dois inteiros cuja diferença é um múltiplo inteiro desse módulo. Mais precisamente, temos a seguinte definição.

Definição 2: Dados um número inteiro positivo *m* e dois inteiros *a* e *b* quaisquer, dizemos que *a* é congruente a *b* módulo *m*, e escrevemos $a \equiv b \pmod m$, se *a – b* é um múltiplo inteiro de *m*.

Por exemplo, $7 \equiv 2 \pmod 5$, já que os restos da divisão de 7 e de 2 por 5 são iguais a 2. Da mesma forma, $19 \equiv 3 \pmod 2$, pois os restos da divisão de 19 e de 3 por 2 são iguais a 1. Outros exemplos de congruência: $-1 \equiv 25 \pmod{26}$, $12 \equiv 0 \pmod 4$.

Classes Residuais: Dado um número inteiro *m > 1*, vamos repartir o conjunto *Z* dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que

possuem o mesmo resto quando divididos por *m*. Isto nos dá a seguinte partição de *Z*:

$$[0] = \{x \in Z;\ x \equiv 0 \pmod m\},$$
$$[1] = \{x \in Z;\ x \equiv 1 \pmod m\},$$
...
$$[m-1] = \{x \in Z;\ x \equiv m-1 \pmod m\}$$

Paramos em $[m-1]$, pois tem-se que $[m] = [0], [m+1] = [1], ...$

O conjunto

$$[a] = \{x \in Z;\ x \equiv a \pmod m\}$$

é chamado de *classe residual módulo m* do elemento *a* de *Z*. O conjunto de todas as classes residuais módulo *m* será representado por Z_m. Portanto,

$$Z_m = \{[0], [1], ..., [m-1]\}.$$

Por exemplo, se *m = 2*, então

$[0] = \{x \in Z;\ x \equiv 0 \pmod 2\} = \{x \in Z;\ x\ é\ par\}$ *e*
$[1] = \{x \in Z;\ x \equiv 1 \pmod 2\} = \{x \in Z;\ x\ é\ ímpar\}.$

Temos também que $[a] = [0]$ se, e somente se, *a* é par e $[a] = [1]$ se, e somente se, *a* é ímpar.

Recíproco ou Inverso Multiplicativo: Na Aritmética usual, cada número não nulo *a* tem um *recíproco*, ou *inverso multiplicativo*, denotado por a^{-1}, tal que

$$a.a^{-1} = 1.$$

Na Aritmética Modular nós temos o seguinte conceito correspondente:

Definição 3: Dado um número *a* em Z_m, dizemos que um número a^{-1} em Z_m é um recíproco, ou inverso multiplicativo de *a* módulo *m* se

$$a.a^{-1} \equiv a^{-1}.a \equiv 1 \pmod m.$$

Pode ser provado que se *a* e *m* não têm fatores primos em comum, então *a* tem um único recíproco módulo *m*. Reciprocamente, se *a* e *m* têm um fator primo em comum, então *a* não tem recíproco módulo *m*.

Exemplos 4: O número 3 tem um recíproco módulo 26, pois 3 e 26 não têm fatores primos em comum. Este recíproco pode ser obtido encontrando o número *x* em Z_{26} que satisfaz a congruência $3x \equiv 1 \pmod{26}$. Embora existam métodos gerais para resolver tais congruências, isto não será abordado aqui, pois nos levaria para muito longe do nosso objetivo. Contudo, como 26 é relativamente pequeno, esta congruência pode ser resolvida por inspeção, testando uma por uma cada solução possível de 0 a 25. Fazendo isto, encontramos que x = 9 é a solução procurada, pois $3.9 = 27 \equiv 1 \pmod{26}$.

Exemplos 5: O número 4 não possui recíproco mod 26, pois 4 e 26 têm o número 2 como fator primo comum.

Para consultas futuras, fornecemos a seguinte tabela de recíprocos mod 26:

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Decifrando a Cifra de Hill: Cada cifra útil deve possuir um procedimento para decifrar. Para decifrar as cifras de Hill, usamos a inversa (*mod 26*) da matriz codificadora. Para ser preciso, se *m* é um inteiro positivo, dizemos que uma matriz *A* com entradas em Z_m é invertível módulo *m* se existir uma matriz *B* com entradas em Z_m tal que

$$A.B = B.A = I \pmod m.$$

Suponha agora que $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ é invertível módulo 26 e que esta matriz é usada para uma 2-cifra de Hill. Se $p=\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ é um vetor comum, então ***c* = *A.p*** é o correspondente vetor cifrado. Para recuperar o vetor ***p*** devemos multiplicar ambos os lados da igualdade anterior por $\boldsymbol{A^{-1}}$ e obter $\boldsymbol{p = A^{-1}.c}$. Assim, cada vetor comum pode ser recuperado do correspondente vetor cifrado pela multiplicação à esquerda por $\boldsymbol{A^{-1}}$ **(*mod 26*)**.

Em Criptografia é importante saber quais matrizes são invertíveis módulo 26 e como obter suas inversas. Em Aritmética comum, uma matriz quadrada *A* é invertível se, e somente se, $\det(A)\neq 0$ ou, equivalentemente, *det (A)* tem um recíproco. O teorema seguinte é análogo deste resultado em Aritmética Modular.

Teorema 6: Uma matriz quadrada *A* com entradas em Z_m é invertível módulo *m* se, e somente se, o resíduo de *det (A)* módulo *m* tem um recíproco módulo *m*.

Como o resíduo de *det (A)* módulo *m* terá um recíproco módulo *m* se, e somente se, este resíduo e *m* não tiverem fator primo em comum, temos o seguinte corolário.

Corolário 7: Uma matriz quadrada *A* com entradas em Z_m é invertível módulo *m* se, e somente se, *m* e o resíduo de *det (A)* módulo *m* não têm fatores primos comuns.

Como os únicos fatores primos de m = 26 são 2 e 13, temos o seguinte corolário que é útil em Criptografia.

Corolário 8: Uma matriz quadrada *A* com entradas em Z_{26} é invertível módulo *26* se, e somente se, o resíduo de *det (A)* módulo *26* não é divisível por 2 ou por 13.

Pode-se demonstrar (porém isto foge ao nosso objetivo) que se $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tem entradas em Z_{26} e se o resíduo de *det (A) = ad – bc (mod 26)* não é divisível por 2 ou por 13, então a inversa de *A (mod 26)* é dada por

$$A^{-1}=(ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}(\text{mod } 26).$$

onde $(ad-bc)^{-1}$ é o recíproco do resíduo de $ad-bc\,(\text{mod } 26)$.

Exemplo 9: Encontre a inversa da matriz $A=\begin{bmatrix} 7 & 5 \\ 5 & 8 \end{bmatrix}(\text{mod } 26)$.

Solução:

$$\det(A)=7.8-5.5=31\equiv 5\,(\text{mod } 26).$$

Usando a tabela de recíprocos (mod 26), encontramos o seu recíproco que é

$$(ad-bc)^{-1}=5.x\equiv 1\,(\text{mod } 26)\Rightarrow x\equiv 21\,(\text{mod } 26)\Rightarrow$$
$$\Rightarrow x=21.$$

Assim, pela fórmula dada, tem-se

$$A^{-1}=(ad-bc)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}(\text{mod } 26)=$$
$$=21.\begin{bmatrix} 8 & -5 \\ -5 & 7 \end{bmatrix}(\text{mod } 26)=$$
$$=\begin{bmatrix} 168 & -105 \\ -105 & 147 \end{bmatrix}(\text{mod } 26)\equiv$$
$$\equiv\begin{bmatrix} 12 & 25 \\ 25 & 17 \end{bmatrix}(\text{mod } 26).$$

Verificando,

$$A.A^{-1}=\begin{bmatrix} 7 & 5 \\ 5 & 8 \end{bmatrix}\begin{bmatrix} 12 & 25 \\ 25 & 17 \end{bmatrix}=\begin{bmatrix} 84+125 & 175+85 \\ 60+200 & 125+136 \end{bmatrix}=$$
$$=\begin{bmatrix} 209 & 260 \\ 260 & 261 \end{bmatrix}\equiv\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}(\text{mod } 26).$$

Analogamente, $A^{-1}.A = I \pmod{26}$.

Exemplo 10: Decifre a *2-cifra de Hill* criptografada no exemplo 1.

Solução:

A mensagem cifrada é "GCMQGLIWKAPA", cujo equivalente numérico é (7; 3), (13; 17), (7; 12), (9; 23), (11; 1), (16; 1). Para obter os pares de texto comum nós devemos multiplicar cada vetor cifrado pela inversa de *A (mod 26)*, ou seja,

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}7\\3\end{bmatrix} = \begin{bmatrix}159\\226\end{bmatrix} \equiv \begin{bmatrix}3\\18\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}13\\17\end{bmatrix} = \begin{bmatrix}581\\614\end{bmatrix} \equiv \begin{bmatrix}9\\16\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}7\\12\end{bmatrix} = \begin{bmatrix}384\\379\end{bmatrix} \equiv \begin{bmatrix}20\\15\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}9\\23\end{bmatrix} = \begin{bmatrix}683\\616\end{bmatrix} \equiv \begin{bmatrix}7\\18\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}11\\1\end{bmatrix} = \begin{bmatrix}157\\292\end{bmatrix} \equiv \begin{bmatrix}1\\6\end{bmatrix} \pmod{26}$$

$$\begin{bmatrix}12 & 25\\25 & 17\end{bmatrix}\begin{bmatrix}16\\1\end{bmatrix} = \begin{bmatrix}217\\417\end{bmatrix} \equiv \begin{bmatrix}9\\1\end{bmatrix} \pmod{26}.$$

pela tabela dada (tabela de associação alfabeto-numérica), os equivalentes alfabéticos destes vetores são: CR – IP – TO – GR – AF – IA, que nos fornecem a mensagem: "CRIPTOGRAFIA".

Agora é com você: Imagine que você é o comandante de uma tropa que está posicionada no campo de batalha e aguarda seus comandos, usando a *2-cifra de Hill* e a matriz codificadora $A = \begin{pmatrix}7 & 5\\1 & 8\end{pmatrix}$, você deseja codificar a frase: "ATACAR AO AMANHECER" e enviá-la para suas tropas de maneira segura. Observe que após agrupar o texto comum em pares de letras e adicionar a letra fictícia no final, obtemos: AT – AC – AR – AO – AM – AN – HE – CE – RR. Usando a tabela de associação alfabeto-numérica, encontramos o equivalente numérico: (1; 20) – (1; 3) – (1; 18) – (1; 15) – (1; 13) – (1; 12) – (8; 5) – (3; 5) – (18; 18). Para codificar os pares do texto comum devemos efetuar o produto da matriz ***A*** por cada um dos vetores correspondentes ao pares de letras dados (vetor ***p***). Não se esqueça que os elementos da matriz produto (vetor ***Ap***) obtida que forem maiores ou iguais a 26 deverão ser substituídos pelos módulos de sua congruência (mod 26), ou seja, devemos tomar o resto de sua divisão por 26, procedendo dessa forma sempre teremos uma associação da mensagem original com letras da tabela de associação dada, isto é, sempre teremos uma mensagem que pode ser transformada em letras do nosso alfabeto.

a) Após codificar a frase dada no enunciado, quais os vetores ***Ap*** correspondentes à codificação? Como fica a frase codificada?

b) Suponha que você recebeu a frase codificada do item anterior, como você faria para decodificá-la? Você seria capaz de encontrar a matriz decodificadora $A^{-1} \pmod{26}$?

c) Quais os conceitos matemáticos envolvidos nos processos de codificação e decodificação da mensagem dada?

d) Crie uma mensagem curta e, usando a matriz ***A***, codifique-a e a envie para outro grupo de sua escolha;

e) Decodifique a mensagem que seu grupo recebeu, utilizando a matriz $A^{-1} \pmod{26}$.