

UNIVERSIDADE FEDERAL DE PERNAMBUCO-UFPE
CENTRO ACADÊMICO DO AGRESTE-CAA
NÚCLEO DE FORMAÇÃO DOCENTE-NFD
CURSO DE MATEMÁTICA-LICENCIATURA

**O USO DA CRIPTOGRAFIA NO PROCESSO DE ENSINO E APRENDIZAGEM EM
FUNÇÕES E MATRIZES NO ENSINO MÉDIO.**

PAULA MIRELY PEREIRA DA SILVA

CARUARU, 2015

PAULA MIRELY PEREIRA DA SILVA

**O USO DA CRIPTOGRAFIA NO PROCESSO DE ENSINO E APRENDIZAGEM EM
FUNÇÕES E MATRIZES NO ENSINO MÉDIO.**

Projeto de Trabalho de Conclusão de Curso,
apresentado à disciplina TCC II, como
requisito obrigatório para a obtenção do título
de licenciada em Matemática pela
Universidade Federal de Pernambuco- Campus
Acadêmico do Agreste.

Orientadora: Kátia Silva Cunha

Coorientadora: Maria Do Desterro A. da Silva

CARUARU, 2015

Catálogo na fonte:
Bibliotecária - Simone Xavier CRB/4-1242

S586u Silva, Paula Mirely Pereira da.
O uso da criptografia no processo de ensino e aprendizagem em funções e matrizes no ensino médio. / Paula Mirely Pereira da Silva. - Caruaru: O Autor, 2015.
79f. il. ; 30 cm.

Orientadora: Kátia Silva Cunha.
Monografia (Trabalho de Conclusão de Curso) – Universidade Federal de Pernambuco, CAA, Licenciatura em Matemática, 2015.
Inclui referências bibliográficas

1. Criptografia. 2. Ensino e aprendizagem. 3. Funções. 4. Matrizes. I. Cunha, Kátia Silva. (Orientadora). II. Título

371.12 CDD (23. ed.) UFPE (CAA 2015-242)



UNIVERSIDADE FEDERAL DE PERNAMBUCO
Centro Acadêmico do Agreste
Núcleo de Formação Docente
Curso de Matemática - Licenciatura



**O USO DA CRIPTOGRAFIA NO PROCESSO DE ENSINO E APRENDIZAGEM EM
FUNÇÕES E MATRIZES NO ENSINO MÉDIO**

PAULA MIRELY PEREIRA DA SILVA

Monografia submetida ao Corpo Docente do Curso de MATEMÁTICA - Licenciatura do Centro Acadêmico do Agreste da Universidade Federal de Pernambuco e **Aprovada** em 09 de dezembro de 2015.

Banca Examinadora:

Profa. Kátia Silva Cunha (CAA - UFPE)
(Orientadora)

Profa. Maria do Desterro Azevedo da Silva (CAA-UFPE)
(Coorientadora)

Profa. Simone Moura Queiroz (CAA-UFPE)
(Examinador Interno)

Prof. Edelweis José Tavares Barbosa (CAA-UFPE)
(Examinador Interno)

DEDICATÓRIA

Dedico este trabalho a minha família que sempre se fez muito importante na minha vida pessoal e acadêmica.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me iluminado em toda a minha vida acadêmica e principalmente na realização desta pesquisa. Um grande agradecimento aos meus pais que sempre estiveram comigo em todos os momentos desde o início da minha vida acadêmica até agora, sempre me apoiando e incentivando em todos os obstáculos que apareceram ao decorrer destes anos. A meus irmãos que da forma que podiam me ajudaram para realização desse sonho, obrigada!!!

Meu muito obrigado também a todos os meus amigos que participaram de grandes fases em minha vida, em particular a Jaqueline, Juliara, Jessica, Mariana, Tatiane, Thamyres que sempre estiveram me ajudando e auxiliando nos estudos. O meu obrigado também vai para minha amiga Ismaelle que me ajudou muito, em momentos muito difíceis para mim, tendo uma grande contribuição para a conclusão deste trabalho, meu muito obrigado Ismaelle. Não poderia esquecer-se de agradecer a meus amigos Cesar, Alex, Anderson que se fizeram também muito significativos aos meus estudos, sempre muito atenciosos e receptivos, não teria chegado aonde eu cheguei sem a ajuda de vocês meninos, meu muito obrigado.

Agradeço também as minhas professoras desde o ensino fundamental que plantaram suas contribuições na minha aprendizagem, e especificamente a minha coorientadora Maria Do Desterro que sempre esteve disponível para contribuir academicamente para o meu trabalho, trazendo suas ideias e melhorias para o trabalho, meu muito obrigado!

Neste mesmo sentido agradecerei a minha orientadora Kátia Silva, que contribuiu muito para a conclusão do meu trabalho, sempre tendo uma imensa paciência comigo e me tranquilizando em momentos difíceis!!! Minha eterna gratidão professora.

RESUMO

Este trabalho refere-se a um estudo sobre a contribuição da criptografia em relação aos conteúdos de Função e Matrizes no Ensino Básico. Trazendo um pouco da historicidade da Criptografia e a mesma relacionada aos conteúdos supracitados, foi observada a contribuição desta para o ensino aprendizagem dos alunos. Para isso, realizamos duas intervenções a partir da aplicação de duas atividades para 16 alunos de uma turma de 3º ano do ensino médio da Escola Cônego Fernando Passos de Passira-PE. Estes momentos de intervenção foram realizados para que os conceitos acerca dos conteúdos em questão fossem revistos, e assim posteriormente aplicados ao estudo de criptografia. A pesquisa foi desenvolvida a partir da abordagem qualitativo, evidenciando uma relação mais social com o indivíduo, analisando o seu discurso minuciosamente através da teoria de análise do discurso de Fairclough. A partir da ampliação das relações que a Matemática pode oferecer para o contexto social, verificamos que a Criptografia pode ser um facilitador no processo de Ensino Aprendizagem desde que os professores a utilizem de forma a complementar o ensino, ou seja, utilizando a Criptografia para auxiliar a ensino, tendo em vista que os alunos já tenham adquirido o conhecimento dos conteúdos. Dessa forma, a pesquisa contribui de um modo geral em relação a diversificar o Ensino Aprendizagem dos conteúdos em sala de aula, proporcionando o aluno a identificar dimensões diferentes do mesmo conteúdo onde ele pode ser utilizado para diversas formas.

Palavras-chave: Criptografia; Ensino e Aprendizagem; Funções e Matrizes.

ABSTRACT

This work refers to a study about the contribution of the encryption in relation to the function of content and matrices in basic education. Bringing a bit of the historicity of encryption and the same related to the above content, was observed the same contribution to the teaching and learning of students. For this, we made two interventions from the application of two activities for 16 students in a class of third year of high school at the School Cônego Fernando Passos in Passira-PE. These intervention moments were carried out so that the concepts about the content in question were reviewed, and so were later applied to the encryption of study. The research was developed from a qualitative approach, showing a more social relationship with the individual, analyzing his speech by analyzing theory of Fairclough. From the expansion of relations that mathematics can offer to the social context, we find that encryption can be a facilitator in the learning process of teaching if the teachers to use in order to complement teaching, ie using encryption to help the school, in order that students have already acquired knowledge of the contents. Thus, the research contributes in general in relation to diversify the teaching and learning of the contents in the classroom, providing students to identify different dimensions of the same content where it can be used for various forms.

Keywords: Cryptography; Teaching and learning; Functions and matrices.

LISTA DE FIGURAS

Figura 1: Resposta do aluno <i>A1</i> em relação a questão 4.a	52
Figura 2: Resposta do aluno <i>A4</i> em relação a questão 4.a	52
Figura 3: Resposta do aluno <i>A1</i> em relação a questão 4.b	53
Figura 4: Resposta do aluno <i>A4</i> em relação a questão 4.b.....	53
Figura 5: Resposta do aluno <i>A1</i> em relação a questão 5.a.....	54
Figura 6: Resposta do aluno <i>A4</i> em relação a questão 5.a.....	54
Figura 7: Resposta do aluno <i>A1</i> em relação a questão 5.b.....	55
Figura 8: Resposta do aluno <i>A4</i> em relação a questão 5.b	55
Figura 9: Resposta do aluno <i>A1</i> em relação a questão 5.c	56
Figura 10: Resposta do aluno <i>A4</i> em relação a questão 5.c.....	56
Figura 11: Resposta do aluno <i>A'10</i> em relação a questão 1.....	63
Figura 12: Resposta do aluno <i>A'9</i> em relação a questão 1.....	63
Figura 13: Resposta do aluno <i>A'10</i> em relação a questão 2	65
Figura 14: Resposta do aluno <i>A'9</i> em relação a questão 2.....	65

LISTA DE QUADROS

Quadro 1. Cifra Atbash.....	17
Quadro 2. Cifra Alban.....	17
Quadro 3. Cifra Atbash.....	17
Quadro 4. Cifra de César.....	18
Quadro 5. Cifra de Alberti.....	19
Quadro 6. Quadrado de Vigenére.....	20
Quadro7. Cifra de Hill.....	22
Quadro 8.Cifra de substituição da Pesquisa.....	29

LISTA DE TABELAS

Tabela 1. Mapeamento da primeira questão sobre a relação de contribuição conforme os entrevistados.....	47
Tabela 2. Mapeamento da segunda questão sobre a relação de contribuição conforme os entrevistados.....	48
Tabela 3. Mapeamento da terceira questão sobre a relação de contribuição conforme os entrevistados.....	50
Tabela 4. Mapeamento da primeira questão sobre a relação de contentamento conforme os entrevistados.....	58
Tabela 5. Mapeamento da segunda questão sobre a relação de contentamento conforme os entrevistados.....	60
Tabela 6. Mapeamento da terceira questão sobre a relação de contentamento conforme os entrevistados.....	61

SUMÁRIO

INTRODUÇÃO	14
1 A CRIPTOGRAFIA VISTA COM UM OLHAR HISTÓRICO	18
1.1 CIFRAS HEBRAICA.....	19
1.2 CIFRA DE CESÁR.....	19
1.3 CIFRA DE AL-KINDIN.....	20
1.4 CIFRA DE ALBERT.....	20
1.5 QUADRO DE VIGENÉRE.....	21
1.6 CIFRA MONOFÔNICA.....	23
1.7 DISCO DE CIFRAS.....	23
1.8 CIFRÁRIO DE FRANCIS BACON.....	23
1.9 ENIGMA.....	24
1.10 CIFRA DE HIL.....	24
1.11 COLOSSUS.....	25
1.12 LUCIFER.....	25
1.13 CIFRA SIMÉTRICA.....	26
1.14 CIFRA ASSIMÉTRICA.....	26
2 A CRIPTOGRAFIA APLICADA A MATEMÁTICA NO ENSINO MÉDIO	27
2.1 MATERIAL INTRODÚTORIO PARA A APLICAÇÃO DA CRIPTOGRAFIA EM FUNÇÕES.....	28
2.1.1 Definições relevantes de funções para o uso da criptografia	29
2.2 MATERIAL INTRODÚTORIO PARA A APLICAÇÃO DA CRIPTOGRAFIA EM MATRIZES.....	32
2.2.1 Definições relevantes para o uso da criptografia em matrizes	32
3 ESTUDO BIBLIOGRÁFICO	37
4 METODOLOGIA DA PESQUISA	41
5 ANÁLISE E RESULTADOS	46

5.1 ANÁLISE DESCRITIVA DA PRIMEIRA ATIVIDADE.....	46
5.2 ANÁLISE DESCRITIVA DA SEGUNDA ATIVIDADE.....	58
5.3 ANÁLISE COMPARATIVA DA PRIMEIRA E SEGUNDA ATIVIDADE.....	67
CONSIDERAÇÕES FINAIS.....	69
REFERÊNCIAS BIBLIOGRÁFICAS.....	71
APÊNDICE 1.....	74
APÊNDICE 2.....	75
APÊNDICE 3.....	76
APÊNDICE 4.....	79

INTRODUÇÃO

Ao discorrer sobre Criptografia, são raras pessoas que a relacionam com algo cotidiano, ou ainda mais com conteúdos vivenciados no Ensino Médio. A Criptografia fornece uma forma interessante e atual de se trabalhar determinados conteúdos de Matemática com os alunos, habituando-os a relacionar o conteúdo puramente matemático com situações que se é comum nos dias atuais.

Com a Criptografia conseguimos proporcionar uma grande conexão com os conteúdos matemáticos e as vivências cotidianas, contribuindo também no melhoramento de competências na forma de resolver problemas, e criar novas formas de resolução, tendo astúcia e um melhor desenvolvimento intelectual durante o processo de aprendizagem (GROENWALD e FRANKE, 2008).

A respeito disso, podemos ver que a Criptografia pode contribuir positivamente para os conceitos matemáticos e o desenvolvimento intelectual no processo de ensino em sala de aula. Esta, segundo Silva, possui além de um envolvimento matemático um contexto histórico repleto de significação, observe:

A Criptografia é tão antiga quanto a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalhas. O mais interessante é que a tecnologia de Criptografia não mudou muito até meados deste século. Depois da segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de mensagens. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna. (SILVA, 2008, p. 137).

A Criptografia é uma ciência antiga utilizada por diversos motivos, entre eles podemos citar os segredos de guerra designados pelos reis ou governantes. Estes procuravam enviar, com sigilo, mensagens secretas para os exércitos onde apenas o remetente e o destinatário sabiam o real significado da mensagem. Com o passar do tempo às necessidades foram se modificando, e os códigos cada vez mais se aperfeiçoando para garantir proteção. Vê-se então que o estudo da Criptografia remonta aos primórdios, e sendo vista até os dias atuais. Atualmente encontramos a Criptografia relacionada a códigos bancários, a transações de correios, assinatura digital, certificado digital, no código de verificação do ISBN, nos navegadores de Internet à aplicações matemáticas, entre outros espaços.

Ao notar o grande valor histórico da Criptografia e suas contribuições no campo social desde décadas passadas, e como além dessa característica de contribuição social a Criptografia também possui uma grande colaboração em relação à Matemática, assim, nada mais natural que introduzi-la no cotidiano da sala de aula. Segundo, Cantoral et al(2000, p.35) “a criptografia pode ser um elemento motivador para o processo de ensino da Matemática” .

É predominante nas aulas de Matemática às listas, as questões com operações complexas que utiliza Frações, Algoritmos, Cálculo com várias Incógnitas, Funções, Matrizes entre outros conteúdos. Estes são de extrema importância para o desenvolvimento do conhecimento da Matemática pura, mas que não possuem um cunho motivador, que consiga envolver o interesse do aluno para obtenção de um ensino e aprendizagem diferenciada. (LIMA, 1999).

Há muito tempo vemos pesquisas que falam sobre novas formas e projeções com ideias vindouras para a educação Matemática (D’AMBROSIO, 1987; 1998) e que estas possuem um papel importante na Matemática com reflexos na educação na chamada sociedade do conhecimento (D’AMBROSIO, 1995).

A referente pesquisa possui como problemática a indagação de como a Criptografia envolverá a resolução das atividades feitas pelos alunos, observando se esta é realmente forma de trabalhar os conteúdos proveitosos para o desenvolvimento pedagógico dos mesmos, se haverá contribuições para o ensino dos conteúdos que são abordados. Seguindo esta Problemática a questão orientadora apresentada neste trabalho é: Quais as implicações que o estudante do ensino médio terá ao relacionar o uso de Criptografia aos conteúdos de Funções e Matrizes?

Alega-se estudar e conhecer como a Criptografia se faz interessante e presente na vida moderna, tendo em vista também toda a sua historicidade, trazendo familiaridade com suas aplicações na Matemática. Existe conveniência em estudá-la para que se consiga absorver os conteúdos do ensino médio de forma mais satisfatória e agradável, com aplicações que possam ser utilizadas no cotidiano. Segundo Tamarozzi (2001) este tema coloca a disposição do professor atividades e jogos de codificação e decodificação envolvendo conteúdos matemáticos que são trabalhados no Ensino Médio e até no Ensino Fundamental II. Escolhendo assim o tema para ser trabalhado com os alunos com o intuito de produzir uma relação positiva entre o ensino do professor em relação a uma aprendizagem motivadora para os alunos.

Como objetivo geral, esta pesquisa tem a intenção de analisar as implicações do uso da Criptografia em sala de aula, com respeito ao estudo de Matrizes e Funções. Fazendo com que tanto o professor quanto os alunos consigam visualizar a importância da aplicação para um ensino motivador. Os objetivos específicos são: Verificar as dificuldades dos discentes diante a Matrizes e Funções. Identificar por meio das atividades as possíveis contribuições que a Criptografia pode oferecer para o ensino e aprendizagem de Funções e Matrizes no ensino médio. Analisar a partir dos dados coletados nos momentos de intervenção, a viabilidade da utilização da Criptografia na construção dos conhecimentos sobre Funções e Matrizes no Ensino e Aprendizagem.

É por meio desses objetivos e pretensões que nosso trabalho será fundamentado. Além disso, temos uma questão que está relacionada diretamente com a nossa pesquisa como: A Criptografia consegue motivar o aluno a dar significado aos conteúdos que são estudados em sala de aula? E a partir desse questionamento levando em consideração que ao introduzir a Criptografia os alunos anteriormente já devem ter um conhecimento prévio sobre o assunto que nossa pesquisa esta centrada.

A metodologia desta pesquisa se dará por intervenções seguidas de atividades que serão respondidas pelos alunos envolvidos no estudo. Tais etapas foram realizadas do seguinte modo: Primeiramente foi preparada uma intervenção para os alunos sobre os conteúdos de Função e Matrizes, revisando os conceitos e colocando alguns exemplos para explicação, depois foi aplicado uma atividade para que os alunos respondessem. A segunda intervenção ocorreu em outro dia, dessa vez foi posto para os alunos uma aula sobre Criptografia e sua relação com a Matemática e alguns exemplos sobre essa aplicação. Após esses dois momentos foi utilizado o teoria do teórico Norman Fairclough que discorre sobre a análise do discurso, para servir de suporte para análise dessas atividades, colocando as descrições sobre as análises e resultados obtidos.

Como referencial teórico para esta pesquisa, demos atenção aos argumentos e posicionamentos de múltiplos doutrinadores e pesquisadores como: Meireles (2001), Rodrigues (2013), Pereira (2012), Fairclough (2001).

Esta pesquisa evidencia a Criptografia como uma aplicação que pode ser utilizada nas aulas do ensino médio por possuir atividades relevantes sobre a disciplina, possibilitando que a aula tenha um cunho mais produtivo e motivador. A fim de detalhar o nosso trabalho o dividimos nos seguintes capítulos: O Capítulo 1 discursará sobre o contexto histórico do desenvolvimento da Criptografia com suas definições e avanços obtidos com o passar do

tempo. No Capítulo 2 será feita uma fundamentação Matemática aplicada à Criptografia no Ensino Médio com exemplos e explicações. O Capítulo 3 refere-se ao estudo bibliográfico do tema, contendo estudos que serviram de base para a pesquisa. No capítulo 4 apresentaremos a metodologia do trabalho com suas especificidades e explicações. Por fim, no Capítulo 5 serão realizadas as análises da pesquisa acrescidas com figuras e discursões sobre as resoluções dos alunos, fazendo um levantamento sobre a relevância do uso da criptografia aos conteúdos de Função e Matrizes.

1 A CRIPTOGRAFIA VISTA COM UM OLHAR HISTÓRICO.

Neste capítulo falaremos brevemente sobre a história da Criptografia, como ela foi surgindo com o passar dos tempos, as diversas utilidades a que foi submetida e seus avanços que sempre foram remetidos em prol de uma melhor qualidade no sigilo das mensagens enviadas.

A Criptografia surgiu em meio à estenografia, que utilizavam maneiras de esconder à mensagem enviada com uso de diferentes estratégias que dificultavam o acesso à mensagem por receptadores. A respeito da estenografia Singh (2003) diz que:

A comunicação secreta, quando é obtida através da ocultação da mensagem, é conhecida como esteganografia, nome derivado das palavras gregas steganos, que significa coberto, e graphein, que significa escrever. Nos dois mil anos que se passaram desde Heródoto, várias formas de esteganografia foram usadas no mundo (SINGH, 2003, p.21).

Com o avanço das populações, foi necessário o avanço das formas de se ter mais segurança no envio das mensagens, assim se desenvolvendo e gerando novas formas de proteção, até chegarmos aos primeiros registros de uso da criptografia, que a partir de Singh (2003, p.22) tem-se que a “[...] criptografia, derivada da palavra grega Kriptos, significa oculto. O objetivo da Criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado [...]” Shokranian, comenta sobre a Criptografia:

Criptografia é um dos tópicos mais antigos do conhecimento. Ela existia, não necessariamente como uma ciência, mas como um conhecimento, principalmente nos assuntos de natureza militar (guerras, armamentos) ou nos assuntos políticos para transmitir informações secretas, mantê-las em segredo e em segurança contra as fontes não autorizadas, como inimigos, espiões, espionagens, etc.(SHOKRANIAN, 2005, p.32).

Por mais, detalharemos alguns tópicos que foram e são importantes no decorrer da criptografia ao passar dos anos.

1.1 CIFRAS HEBRAICAS.

Desde a Antiguidade os hebreus possuíam interesse em mensagens secretas, para tal utilizavam as cifras Atbash, Albam e Atbah, para se comunicar de forma segura. Na cifra Atbash, a primeira letra do alfabeto é substituída pela última, a segunda letra pela penúltima e assim sucessivamente, como se pode observar abaixo:

Quadro-1. Cifra Atbash

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

Fonte: o autor, 2015.

Também existia a cifra de substituição chamada de Albam, esta é obtida da seguinte forma: a primeira letra é substituída pela que ocupa 14^a posição, a segunda letra pela que ocupa a 15^a, até a 13^a letra ser substituída pela 26^a. Vejamos o quadro abaixo:

Quadro-2. Cifra Albam

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

Fonte: o autor, 2015.

A cifra Atbah, segue a linha de raciocínio das cifras acima. O nome Atbah tem a seguinte origem: a primeira letra do alfabeto hebreu (Aleph) é trocada por Teth e a segunda (Beth) é trocada por Heth. Logo, Aleph Teth Beth Heth originou ATBAH. Observemos a representação da cifra abaixo:

Quadro-3. Cifra Atbah

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

Fonte: o autor, 2015.

1.2 CIFRA DE CÉSAR.

Existem alguns contatos com a Criptografia propriamente dita na Grécia utilizada pelo militar e governante romano Júlio César (100 a.C. - 44 a.C.), na época da transição do final do período republicano da Roma Antiga. Júlio César utilizava-se da criptografia com finalidades

militares devido à segurança que este procedimento proporcionava. No livro “As vidas dos Césares”, escrito no século II por Suetônio, neste escrito descreve os recursos utilizados por César, consistia numa substituição de cada letra do alfabeto por outra três posições adiante, a partir do que as três últimas letras do alfabeto fazem corresponder às três primeiras. Na prática, a letra “a” era substituída pela letra “d”; a letra “b”, pela “e”; a letra “c”, pela “f” e assim sucessivamente (MARQUES, 2013). Note como o alfabeto da língua portuguesa ficaria representado após a cifra de César.

Quadro- 4. Cifra de César

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

Fonte: (SINGH, 2003, p.27)

Para decifrar a cifra de César é necessário deslocarem as ordens das letras do texto em c três posições para a esquerda, chegando assim ao texto inicial.

1.3 CIFRA DE AL-KINDIN.

Muitos estudiosos árabes conseguiram chegar a teorias sobre a cifra de substituição, onde elas não eram de fato tão inabaláveis, notando-se certa frequência no seu uso. Utilizando o procedimento de cifrar de Al-kindin, é necessário conhecer o idioma da mensagem codificada. Para realizar o processo de codificação é obrigatório se ter um texto suficientemente grande que ocupe uma página onde é possível fazer a análise de sua frequência.

Em seguida fazendo uma tabela com a frequência relativa das letras que foram aparecendo, com os valores da tabela anterior, substituindo as letras pelas as letras da tabela que tem percentagens iguais, até que a mensagem fique clara, ou seja, possível de leitura.

1.4 CIFRA DE ALBERT.

Leon Batista Alberti nascido em 1404, conhecido como grande arquiteto que foi destaque na renascença, também importante escritor sobre as práticas de cifragem. Albert escreveu um ensaio do que acreditava ser um novo tipo de cifra. Conseguindo propor a

utilização de dois ou mais alfabetos cifrados, usados alternadamente, para atrapalhar os criptoanalistas. No qual podemos observar na seguinte tabela:

Quadro-5. Cifra de Alberti

Alfabeto original	A	b	C	D	E	F	G	H	I	J	K	L	M	N	C	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado 1	X	F	O	R	I	H	J	K	N	G	M	E	Z	B	Y	P	A	L	Q	D	C	T	U	S	V	W
Alfabeto cifrado 2	F	R	O	A	L	M	E	G	H	I	J	K	N	P	Y	Z	B	C	D	Q	S	T	U	V	W	X

Fonte: o autor, 2015.

E este método, houve avanços significativos em relação a não permitir que a mesma letra do texto original apareça como uma única letra do alfabeto cifrado, ou seja, sendo ele o primeiro a utilizar a cifra de substituição polialfabética.

1.5 QUADRADO DE VIGENÉRE

A cifra de Vigenére composta por 26 alfabetos cifrados seletos para criar a mensagem cifrada. Pois quanto mais alfabetos utilizados, maior seria o grau de dificuldade empregado no método, para criar uma cifra mais complexa. A cifra de Vigenére conseguia dificultar a recepação por meio da sua grande diversidade de alfabetos empregados a partir de sequências distintas. Abaixo podemos evidenciar como a cifra de Vigenére conhecida como “quadrado de Vigenére” se comportava:

Quadro-6. Quadrado de Vigenére.

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

Fonte:(SINGH ,2003, p. 66)

Observando o quadrado de Vigenère, notamos que a primeira fileira é constituída por um alfabeto cifrado com a cifra de César, com deslocamento de uma letra na sequência do alfabeto. A segunda fileira constitui-se da mesma forma, porém com um deslocamento de duas casas e assim por diante para as outras fileiras. Nesta cifra utiliza-se uma linha diferente do quadrado para codificar letras diferentes da mensagem. Para decifrar a mensagem enviada precisava saber que linha do quadrado de Vigenère foi usada para a cifragem, daí utiliza-se uma palavra-chave. Como esta cifra é polialfabetica fica protegido contra a análise de frequências, tendo assim mais segurança.

1.6 CIFRAS HOMÓFONICAS

Em 1411, aparecem as primeiras cifras homofônicas com pretensão de dificultar a análise de frequência, introduzindo assim os homófonos e os nulos. Os quais, não estavam ligados a nenhuma letra, eram introduzidos aleatoriamente durante o texto cifrado para embaralhar os criptoanalistas que tentasse analisar os textos secretos.

1.7 DISCOS DE CIFRAS

Na Itália, precisamente no século XV, houve uma grande contribuição na Criptografia devido a grande demanda de diplomatas que lá residiam. Um dos grandes diplomatas Leon Battista Alberti (1404- 1472 d. C) publicou em 1466, o livro *Modus scribendi in ziferas*, onde fala do disco de cifra, uma das primeiras cifras monoalfabeticas.

O disco era constituído de dois discos de cobres, sendo um maior e outro menor. O disco maior era fixo e o outro móvel, contendo o alfabeto na sua borda. Porém no alfabeto não estava incluso as letras H, J, K, U, W e Y; nos espaços das letras que sobraram colocou os algarismos 1, 2, 3 e 4. No disco menor a vigésima quarta letra o & (et) e este representa o alfabeto de cifra.

Outro disco muito utilizado criado por Alberti, também constituído de dois discos, sendo um disco maior fixo e outro menor móvel. Porém neste caso na borda dos discos havia apenas os alfabetos no disco maior o alfabeto maiúsculo e no disco menor o alfabeto minúsculo. Esse disco foi muito utilizado na guerra civil americana, tendo muito êxito e eficácia para transmitir as mensagens com segurança.

1.8 CIFRÁRIO DE FRANCIS BACON

Um filósofo inglês chamado Francis Bacon (1561-1626 d. C), criou uma cifra que utilizava apenas duas letras A e B para representar o alfabeto cifrado, e estas duas letras

formavam uma sequencia de cinco letras. Onde a ordem ocorria uma permutação. Como podemos observar:

$$a = AAAAA, b = AAAAB, c = AAABA, d = AAABB$$

e assim analogamente até chegarmos ao

$$z = BABBB$$

1.9 ENIGMA

Em Março de 1918, no final da primeira guerra mundial o exército alemão criou e utilizou a cifra ADFGVX, que era de substituição e ao mesmo tempo de transposição, esta cifra foi desvendada em dois de Junho do mesmo ano, pelo tenente francês Georges Painvin. Utilizou-se de tecnologia do século XX, criando uma máquina criptográfica que era uma versão elétrica do disco de cifras. E a esta lhe deu o nome de Enigma, o mais cruel sistema de Criptografia já visto (SINGH, 2003).

Para que uma mensagem fosse enviada utilizando a Enigma, o emissor girava os misturadores para determinar a posição inicial. Havia 17.576 ajustes possíveis e, assim 17.576 posições iniciais. E esta posição era que determinava como a mensagem seria cifrada, ou seja, era a chave da decodificação.

1.10 CIFRA DE HILL

O sistema de Criptografia polialfabética chamada cifra de Hill foi inventada em 1929 por Lester S. Hill. Este sistema consiste em fazer m combinações lineares dos n caracteres do texto plano, produzindo os m caracteres do texto criptografado. As cifras de Hill são baseadas em transformações matriciais, relacionando cada letra a um numero correspondente. Observe a 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
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

Fonte: o autor, 2015.

1.11 COLOSSUS

Em 1943, outro aparelho foi criado com propósito de decifrar mensagens sendo desenvolvido na Inglaterra com base nas ideias de Turing. Denominado de Colossus, foi usado para decifrar as codificações feitas pela máquina Lorenz, dedicada as mensagens de Hitler e seus generais. Este possuía uma dimensão extraordinária e funcionava por meio de válvulas, que processava cerca de 5 mil caracteres por segundo. A partir da Colossus obteve uma era moderna da Criptografia. Podendo ressaltar que os computadores tiveram origem na criptoanálise, sendo programados com chaves de codificação muito mais complexas.

Na Segunda Guerra Mundial, a planta de construção da Colossus foi queimada. Dando os méritos da construção do computador a outros cientistas. Em 1945, na Universidade da Pensilvânia, foi construído o Electronic Numerical Integrator And Calculator (ENIAC), que possuía 18 mil válvulas eletrônicas que possibilitava realizar cinco mil cálculos por segundo.

1.12 LUCIFER

Em 1970 a IBM lançou o sistema de cifragem conhecido como Lucifer. Esse sistema executa a cifragem da mensagem a partir dos seguintes procedimentos: Inicialmente a mensagem é convertida numa fileira de dígitos binários; em seguida a fileira é dividida em blocos de 64 dígitos, onde acontece a cifragem dos blocos de forma separadamente. Após esses procedimentos, é retirado um bloco de 64 dígitos e destes divididos na metade, e atribuímos os locais onde os blocos irão ficar de esquerdo1 e direito1, passando por uma função “transformadora” que muda os dígitos em relação com a substituição.

O bloco que fica no lado direito é “transformado” e somado ao esquerdo, tendo assim um novo bloco de 32 dígitos que chamamos de direito 2. E o direito1 e recebe o nome de esquerdo1. E repete-se o processo agora utilizando os novos blocos ate atingir 16 vezes. O texto cifrado é então enviado e para decifrar a mensagem o processo é invertido.

Este sistema foi considerado muito forte, possuindo sistemas de decifragem seguros e potentes sendo utilizado por várias organizações. E este ainda seria utilizado como padrão americano se não fosse à interferência da National Security Agency- (NSA). Esta agência antes de possibilitar o uso do Lucifer fez algumas restrições como diminuir seu número de chaves a aproximadamente 56 bits, liberando o uso em 23 de novembro de 1976, e batizando o Lúclifer de DES (Data Encryption Standart), ou seja, (padrão de cifragem de dados).

1.13 CIFRA SIMÉTRICA

A Cifra Simétrica tem objetivo de transformar um texto normal sucinto em um texto cifrado, fazendo uso de chaves secretas e algoritmos de criptografar. Para esta cifra medimos o seu poder pelo tamanho da sua chave, ou seja, quanto maior melhor. Geralmente as chaves de 40 bits eram consideradas as mais fáceis de decodificar e as mais fortes possuíam 256 bits, ou mais. A partir da chave inicial e com o uso de um algoritmo de criptografar o texto é recuperado a partir do texto cifrado, não possuindo muita segurança dado que as chaves ficam vulneráveis e muitas vezes eram cifradas a mensagem por pessoas não desejadas.

1.14 CIFRA ASSIMÉTRICA

A Cifra Assimétrica inventada por Whitfield Diffie nascido em Nova Iorque, estados unidos da América em 1944. Especialista em segurança da informação trabalhador sem vínculos com o governo, trabalhando independentemente criou uma cifra, cujo nomeou com seu nome Diffie, esta se utilizava de uma chave para cifrar uma mensagem e usar uma diferente para decifrá-la sendo isto uma grande inovação, pois até naquela época só se usava cifras simétricas, onde usavam a mesma chave para cifrar e decifrar uma mensagem.

2 A CRIPTOGRAFIA APLICADA A MATEMÁTICA NO ENSINO MÉDIO.

Trataremos de introduzir a Criptografia no ensino dos conteúdos já supracitados neste trabalho, utilizando-se as devidas técnicas Matemáticas para chegar ao resultado desejado. Tendo por vista o envolvimento e a ligação da Criptografia neste contexto escolar, tornando-se mais prazeroso o aprendizado para os alunos. Primeiramente veremos uma breve descrição da Criptografia ligada ao ensino, em seguida será posto detalhadamente o procedimento da aplicação de Criptografia com os conteúdos.

As Funções e Matrizes podem ser utilizadas como chaves codificadoras e decodificadoras, possuindo atividades didáticas, onde o aluno do Ensino Médio aplica os conceitos matemáticos em situações práticas de Criptografia. Impondo o aluno a pensar de forma organizada seus conceitos matemáticos, o colocando em uma situação nova, onde ele requer de processos metodológicos que envolva o referencial teórico com a prática.

Segundo os Parâmetros Curriculares Nacionais para o Ensino Médio (BRASIL, 2000, p.9) “podemos ressaltar a importância da” educação na sociedade tecnológica, bem como, apontam a finalidade do Ensino Médio no artigo 35, parágrafo IV: “a compreensão dos fundamentos científico-tecnológicos dos processos produtivos, relacionando a teoria com a prática, no ensino de cada disciplina”.

De acordo com as Orientações Curriculares para o Ensino Médio (OCEM), temos:

Ao final do Ensino Médio, espera-se que os alunos saibam usar a Matemática para resolver problemas práticos do cotidiano; para modelar fenômenos em outras áreas do conhecimento; compreendam que a Matemática é uma ciência com características próprias, que se organiza via teoremas e demonstrações; percebam a Matemática como um conhecimento social e historicamente construído; saibam apreciar a importância da Matemática no desenvolvimento científico e tecnológico. (BRASIL, 2006, p.69).

A Criptografia pode contribuir positivamente para o ensino, tendo estratégia e funcionalidade para trabalhar tanto a parte das definições e operações, assim como na interligação com o mundo além da sala de aula, onde essas operações podem aparecer de forma questionadora e instigante. Os Parâmetros Curriculares Nacionais para o Ensino Médio comentam:

Tínhamos um ensino descontextualizado, compartimentalizado e baseado no acúmulo de informações. Ao contrário disso, buscamos dar significado ao conhecimento escolar, mediante a contextualização; evitar a compartimentalização, mediante a interdisciplinaridade; e incentivar ao raciocínio e a capacidade de aprender (PCN, 2000, p. 4).

Ainda pelos Parâmetros Curriculares Nacionais para o Ensino Médio, observemos:

No Ensino Médio, quando nas ciências torna-se essencial uma construção abstrata mais elaborada, os instrumentos matemáticos são especialmente importantes. Mas não é só nesse sentido que a Matemática é fundamental. Possivelmente, não existe nenhuma atividade da vida contemporânea, da música à informática, do comércio à meteorologia, da medicina à cartografia, das engenharias às comunicações, em que a Matemática não compareça de maneira insubstituível para codificar, ordenar, quantificar e interpretar compassos, taxas, dosagens, coordenadas, tensões, frequências e quantas outras variáveis houver. (PCN, 2000, p. 9).

O distanciamento dos conteúdos em relação com a realidade e com o contexto do aluno acaba proporcionando um estudo pouco motivador. Onde os mesmos não conseguem fixar os conteúdos dado pelo professor, Segundo Tamarozzi:

O tema Criptografia disponibiliza atividades didáticas que desenvolvem habilidades Matemáticas no conteúdo de Funções e Matrizes que se constituem em material útil para exercícios, atividades e jogos de codificação, onde o professor pode utilizá-los para fixação dos mesmos aos alunos.(TAMAROZZI, 2001, p. 23).

Neste cenário, acreditamos que noções introdutórias de Criptografia podem enriquecer o ensino dos conceitos de Função e Matrizes.

2.1 MATERIAL INTRODUTÓRIO PARA APLICAÇÃO DE CRIPTOGRAFIA EM FUNÇÕES.

Uma das cifras mais simples utilizadas para codificar e decodificar são as cifras de substituição em que cada letra da mensagem é substituída por outra. Porém para o nosso caso precisamente iremos utiliza-la fazendo uso da substituição das letras por números.

Assim, cifrar uma mensagem recai em permutar números por meio de uma regra f . Podendo ser feito de forma muito prática, por exemplo, através das Funções Afins $f(x) =$

$ax + b$, com a, b inteiros, sendo a diferente de zero, definidas no conjunto de 0 á 26 (DRUCK, 2004). Para decifrar esta mensagem faremos uso da Função Inversa da mesma que foi utilizada anteriormente, logo chegando ao resultado desejado, ou seja, de forma geral a aplicação deste se dá em pegar a mensagem original convertê-la em números (codificar) por uma função bijetora e, por sua inversa, transformar (decodificar), os números até chegar á mensagem original.

Para lembrar alguns conceitos veremos as seguintes definições que serão importantes para introdução da aplicação ao conteúdo.

2.1.1 Definições Relevantes de Funções Para o Uso de Criptografia.

Definição 1 Sejam A e B conjuntos diferentes do vazio. Uma relação f de A em B é uma função, se e somente se, qualquer elemento de A estiver associado a um único elemento de B . O conjunto A é chamado domínio da função e o conjunto B contra-domínio, e os que estiver associado a um elemento de A , será chamado de Imagem da função.

Para estabelecer agora a Função Inversa que é a responsável pela decifração veremos as seguintes definições.

Definição 2 Uma função $f: A \rightarrow B$ é dita Injetiva quando elementos diferentes de A são transformados por f em elementos diferentes de B , ou seja, não há elemento em B que seja Imagem de mais de um elemento de A . Assim, f é injetiva quando:

$$x_1 \neq x_2 \text{ em } A \Rightarrow f(x_1) \neq f(x_2) \text{ em } B.$$

Definição 3 Uma função f é Sobrejetiva quando, para qualquer elemento $y \in B$, pode-se encontrar um elemento $x \in A$ tal que $F(x) = y$. Ou seja, f é sobrejetiva quando todo elemento de B é imagem de pelo menos um elemento de A , isto é, quando $Im(f) = B$

Definição 4 Uma função $f: A \rightarrow B$ é Bijetora se ela for, simultaneamente, injetiva e sobrejetiva. Quando isso ocorre dizemos que há uma bijeção ou uma correspondência biunívoca entre A e B .

Definição 5 Dada uma função $f: A \rightarrow B$, Bijetiva, denomina-se função inversa de f a função de $g: B \rightarrow A$ tal que, se $f(a) = b$, então $g(b) = a$, com $a \in A$ e $b \in B$. Sendo representada a função inversa de f por f^{-1} .

Observemos a seguir um exemplo detalhadamente que utiliza esses procedimentos.

Exemplo: Duas colegas de classe chamadas Jéssica e Jaqueline desejam se comunicar em segredo. Para isso determinam uma função que será usada para manter esse segredo, logo a Função escolhida foi $f(x) = 2x + 1$ para codificar a mensagem, porém para utilizar esse modo de codificação Jéssica constrói uma tabela relacionando cada letra do alfabeto a um número e entrega para a Jaqueline. Daí observe a tabela de substituição:

Quadro- 8. Quadro de substituição da pesquisa.

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	26

Fonte: O autor, 2015.

Assim observando a tabela conseguimos enxergar que os valores dos números correspondem ao domínio da função. Desse modo, Jessica tenta cifrar a seguinte mensagem: “PASSEI NA UFPE”. Seguindo os procedimentos ela transformou cada letra em um respectivo número como consta na tabela acima, por exemplo, substituiu a primeira letra P pelo número 16, a letra A por 1 e assim sucessivamente até que todas as letras da mensagem sejam substituídas pelos números. Ou seja, a mensagem irá se encontrar da seguinte forma “16 – 1 – 19 – 19 – 5 - 9 – 14 – 1 – 21 – 6 – 16 – 5”.

Uma vez que o as letras já foram substituídas pelos números Jéssica atribui cada número a Função escolhida para que consiga os valores numéricos que irá utilizar para enviar a mensagem para Jaqueline. Notemos nos seguintes cálculos:

$$f(16) = 2x + 1 = 33$$

$$f(1) = 2x + 1 = 3$$

$$f(19) = 2x + 1 = 39$$

$$f(19) = 2x + 1 = 39$$

⋮

E assim sucessivamente até chegar à seguinte cifra:

$$33 - 3 - 39 - 39 - 11 - 19 - 29 - 3 - 43 - 13 - 33 - 11.$$

Ao receber esta cifra e a função da mesma, Jaqueline calculou a inversa da função e atribuiu cada número a função para chegar a mensagem original, vejamos o decorrer do processo abaixo:

Primeiramente calculamos a função inversa de $f(x) = 2x + 1$, para isso veja:

$$x = 2f(x)^{-1} + 1$$

$$x - 1 = 2f(x)^{-1}$$

$$\frac{x - 1}{2} = f(x)^{-1}$$

Ou seja, $f(x)^{-1} = \frac{x-1}{2}$ é a função inversa da função usada para cifrar a mensagem original.

Logo cada número será posto nessa função para que possamos chegar à mensagem original observe:

$$f(33)^{-1} = \frac{x-1}{2} = 16$$

$$f(3)^{-1} = \frac{x-1}{2} = 1$$

$$f(39)^{-1} = \frac{x-1}{2} = 19$$

$$f(39)^{-1} = \frac{x-1}{2} = 19$$

$$f(11)^{-1} = \frac{x-1}{2} = 5$$

⋮

Assim até obtermos a sequência inicial:

16 – 1 – 19 – 19 – 5 – 9 – 14 – 1 – 21 – 6 – 16 – 5 .

E a partir da sequência obtida, observarmos na tabela e depois fazendo as inferências necessárias até chegar à mensagem original. Nesse exemplo, observamos de forma prática como a Criptografia pode ser inserida no ensino de Função facilmente, pois como essa Função é Polinomial de primeiro grau temos que a Função é Injetora e como o contra domínio será a sequência de valores obtida por Jaqueline, então temos uma Função Bijetora. Porém essa mesma ideia pode ser introduzida em Funções Polinomiais do segundo grau, em Função Exponencial chegando aos mesmos resultados, claro respeitando as suas Inversas.

2.2 MATERIAL INTRODUTÓRIO PARA A APLICAÇÃO DA CRIPTOGRAFIA EM MATRIZES.

Outra forma de manifestação da Criptografia em matemática vê-se no estudo de Álgebra Matricial. Para isto utilizando meios como a multiplicação de Matrizes e Matrizes Invertíveis como chaves, o que faz dificultar a violação da mensagem (DRUCK, 2004). Esta também se utiliza do método de substituição, fazendo com que o aluno execute as operações de forma organizada conseguindo codificar e decodificar a mensagem através desses procedimentos.

Para o decorrer deste tópico 2.2 veremos algumas definições importantes para o desdobramento desta aplicação Criptográfica.

2.2.1 Definições Relevantes Para o Uso de Criptografia em Matrizes.

Definição 1 Uma Matriz é um arranjo numérico formado por linhas e colunas. Possui a seguinte representação: $A_{m \times n} = [a_{ij}]_{m \times n}$, onde m é igual ao número de linhas da matriz, n ao número de suas colunas e a_{ij} o elemento da i -ésima linha e j -ésima coluna. A matriz pode ser denotada por A ou por $[a_{ij}]_{m \times n}$, como pode ser vista na representação abaixo:

$$A_{m \times n} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} = [a_{ij}]_{m \times n}$$

Definição 2

Se $A = [a_{ij}]$ é uma matriz $m \times p$ e $B = [b_{ij}]$ é uma matriz $p \times n$, então o produto de A por B , denotada por AB , é a matriz $C = [c_{ij}]$ de ordem $m \times n$ definida por:

$$c = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj} = \sum_{k=1}^p a_{ik}b_{kj} \quad (1 \leq i \leq m \text{ e } 1 \leq j \leq n)$$

O produto de A por B está definido apenas quando o número de linhas de B é exatamente igual ao número de colunas de A , ou seja,

$$\begin{array}{ccc} A & B & \\ m \times p & p \times m & = & AB \\ & & & m \times n \end{array}$$

Ainda quando o produto AB não é definido se A uma matriz $m \times p$ e B uma matriz $q \times n$, com $p \neq q$.

Definição 3 Dado uma matriz $A_{n \times n}$, esta é dita inversível se e somente se existe uma matriz $B_{n \times n}$, tal que:

$$AB = BA = I$$

Onde I é a matriz identidade. A matriz B , caso exista, chama-se inversa de A e indica-se A^{-1} .

Teorema 1 Se uma matriz tem inversa, então a inversa é única.

Demonstração:

Sejam B e C matrizes inversas de A . Então $BA = AC = I_n$. Assim,

$$B = BI_n = B(AC) = (BA)C = I_n C = C$$

□

Em particular vale que,

$$\det(A^{-1}) = \frac{1}{\det A}$$

A matriz quadrada admite inversa se $\det A \neq 0$, se não for inversível dizemos que a matriz é singular. □

Definição 4 Seja A uma matriz de ordem n . Cujo determinante indicamos por $\det A$ o número que podemos obter operando com os elementos de A da seguinte forma:

No primeiro caso poderemos ter uma matriz A de ordem $n=1$, para este caso temos que o determinante irá ser o seu único elemento, ou seja,

$$A = [a_{11}] = a_{11} \Rightarrow \det A$$

Para $n=2$, temos que o determinante irá se comportar da seguinte forma:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \Rightarrow \det A$$

Para $n = 3$, temos que o determinante é definido da seguinte forma:

$$\begin{aligned} A &= \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \\ &= a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{13} \cdot a_{22} \cdot a_{31} - \\ &\quad a_{11} \cdot a_{23} \cdot a_{32} - a_{12} \cdot a_{21} \cdot a_{33} \Rightarrow \det A. \end{aligned}$$

Descrevemos abaixo um método bastante simples, para codificar e decodificar mensagens, que envolve apenas um par de matrizes de ordem n , A e A^{-1} , cujos elementos devem ser números inteiros.

Exemplo: Marcela irá enviar uma mensagem criptografada para sua mãe. Para isto anteriormente combinaram que ela iria enviar essa mensagem codificada utilizando uma matriz codificadora para isso. A matriz escolhida para ser codificadora foi a seguinte:

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

Esta ainda será utilizada para codificar e decodificar a mensagem que Marcela quer enviar para sua mãe. A mensagem que Marcela irá enviar é a seguinte:

“Passei na UFPE”

Agora para que a mensagem possa ser codificada utilizando este método, Marcela deverá montar uma matriz dois por dois, onde o número de colunas irá ser dependente da quantidade de texto a ser cifrado. Se a mensagem obtiver uma quantidade de letras ímpar a ultima letra da mensagem deverá ser repetida. Assim Marcela primeiramente deverá atribuir um número para cada letra de sua mensagem seguindo a tabela abaixo seguindo o mesmo modelo da Tabela 8, na qual veremos abaixo novamente:

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	26

Fonte: o autor, 2015.

A mensagem após a atribuição aos números resultou em:

“16 – 1 – 19 – 19 – 5 – 9 – 14 – 1 – 21 – 6 – 16 – 5”

Com esta sequência de números Marcela monta sua matriz dois por seis. Observe:

$$M_{2 \times 6} = \begin{bmatrix} 16 & 1 & 19 & 19 & 5 & 9 \\ 14 & 1 & 21 & 6 & 16 & 5 \end{bmatrix}$$

Em seguida calcula o produto da matriz codificadora A com a matriz M . Vejamos abaixo:

$$\begin{aligned} A.M &= \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 16 & 1 & 19 & 19 & 5 & 9 \\ 14 & 1 & 21 & 6 & 16 & 5 \end{bmatrix} \\ &= \begin{bmatrix} 44 & 3 & 61 & 31 & 37 & 19 \\ 104 & 7 & 141 & 81 & 79 & 47 \end{bmatrix} \end{aligned}$$

Que irá se tornar a matriz que possui a mensagem cifrada e a esta atribuímos como matriz C . Logo a mensagem que Marcela irá enviar para sua mãe se dará da seguinte forma:

“44 – 3 – 61 – 31 – 37 – 19 – 104 – 7 – 141 – 81 – 79 – 47”

Para que a mensagem seja codificada a mãe de Marcela deve recuperar a matriz A , utilizando-se a matriz inversa da matriz codificadora, ou seja, temos que calcular a matriz

inversa de A , como $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, tem $A^{-1} = \frac{1}{\det A} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, com $\det A = ad - cd \neq 0$.

Assim $A^{-1} = \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix}$. Com isso podemos fazer a operação codificadora que segue da multiplicação de $A^{-1} \cdot C$. Assim chegamos em:

$$\begin{aligned} \frac{1}{\det A} A^{-1} \cdot C &= -\frac{1}{2} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 44 & 3 & 61 & 31 & 37 & 19 \\ 104 & 7 & 141 & 81 & 79 & 47 \end{bmatrix} \\ &= \begin{bmatrix} 16 & 1 & 19 & 19 & 5 & 9 \\ 14 & 1 & 21 & 6 & 16 & 5 \end{bmatrix} \end{aligned}$$

O que nos remete a mensagem original, substituindo-a pelas suas respectivas letras utilizando a tabela 8, chegamos à mensagem “Passei na UFPE” a qual foi enviada inicialmente por Marcela para sua mãe, e na qual ela conseguiu desvendar corretamente chegando ao resultado esperado por sua filha.

Para este método criptográfico utilizamos operações matriciais simples que não fazem necessidade de nenhum artifício que foge do conhecimento do aluno.

3 ESTUDO BIBLIOGRÁFICO

Ao pesquisar sobre o tema do trabalho foi possível encontrar discussões que fazem referência à abordagem da Criptografia em Funções e Matrizes em estudos atuais. É um assunto ainda pouco discutido em pesquisas, mais a partir dos textos que serão abordados a seguir veremos a sua grande significância para o ensino. Iremos ver neste capítulo algumas discursões referentes ao processo de Ensino e Aprendizagem, com finalidade de colaborar com os estudos que serão feitos posteriores.

Na pesquisa de Meireles (2011), objetivou-se em analisar a utilização da Criptografia relacionada a conteúdos do cotidiano dos alunos sendo uma boa estratégia para o Ensino e Aprendizagem da Matemática. Estabelecendo conexões com o conteúdo Matricial através de uma atividade diferenciada que foi aplicada aos alunos, esta mesma foi desenvolvida para que proporcionassem motivação, criatividade e o desenvolvimento do raciocínio lógico aos alunos. A aplicação da atividade aconteceu na Escola Estadual Ênio Pipino, na cidade de Sinop - MT, na turma do 3º Ano L, do Ensino Médio. A pesquisa realizada foi qualitativa.

No trabalho de Meireles a grande motivação em discutir sobre esse tema foi pelo fato de que atualmente os professores de Matemática encontraram uma grande dificuldade em relacionar alternativas Matemáticas de ajuda do conteúdo abordado em sala de aula de maneira que sejam motivadoras para ascender o interesse dos alunos pelo aprendizado da Matemática.

A mesma foi realizada com a preocupação de investigar se o uso de alternativas diferenciadas, as quais relacionassem um tema atual e do cotidiano com a Matemática, podem contribuir para o desempenho do aprendizado dos alunos. Aonde os mesmos pudessem fazer inferências com o mundo real. Tendo em vista que nossa pesquisa objetiva investigar o processo de aquisição de conceitos, destacamos que investigar um determinado assunto significa coletar informações através de formulação de problemas de uma determinada situação ou tema a ser explorado, utilizando os Parâmetros Curriculares Nacionais para o Ensino Médio (PCN's).

O estudo de Meireles foi de muita importância, pois o mesmo trouxe inovações ao ensino de Matrizes, conseguindo criar atividades atrativas, onde os alunos puderam desenvolver um raciocínio lógico sobre os conteúdos que foram abordados nas atividades, contribuindo para um Ensino e Aprendizagem diferenciado e empolgante.

Na dissertação de Rodrigues (2013), optou em objetivar seu trabalho em facilitar o entendimento do aluno sobre o conteúdo de Funções, utilizando a Criptografia por meio da codificação e decodificação de mensagens. Essa intervenção teve a intenção de ser feita com um cunho mais divertido, aonde o aluno pudesse desenvolver a curiosidade e fazer as investigações da Função que foi utilizada na hora de codificar e decodificar as mensagens.

A metodologia aplicada no trabalho de Rodrigues segue os conceitos de Engenharia didática segundo a teórica Artigue (1996). Que fala sobre o desenvolvimento de uma metodologia embasada na Engenharia Didática.

A pesquisadora organizou sua pesquisa da seguinte forma. Na primeira etapa foi feita uma análise das dificuldades mais relevantes que os alunos possuíam, e embasados nessas dificuldades foram elaboradas 9 atividades que foram aplicadas na sala de aula. Na segunda etapa foi desenvolvido um experimento com 12 alunos do 9º ano, do Ensino Fundamental, da escola estadual João Urias da Silva, do município de Águas da Prata, estado de São Paulo. As atividades foram desenvolvidas em 4 aulas, distribuídas em dois dias letivos. Os conteúdos das atividades didáticas aplicadas, desenvolvidas no experimento foram: Criptografia, Função e suas especificidades. Os dados foram coletados a partir da observação e das atividades que foram feitas pelos alunos, e estes foram organizados em duplas que lhe foi atribuído o nome de A, B, C, D, E e F.

Ao finalizar sua pesquisa Rodrigues constatou que o envolvimento da Criptografia com o conteúdo de Funções foi um método eficaz e positivo para o Ensino e Aprendizagem, pois foi capaz de levar o aluno a atribuir significado ao conceito de Função no fim do Ensino Fundamental. Além de proporcionar ao professor maneiras de contextualizar os assuntos em sala de aula, ajudando a revisar, e fixar o estudo de Funções para os alunos.

Ao vermos a pesquisa de Rodrigues, acreditamos de fato que são grandes os procedimentos que podem ser vivenciados em sala de aula e que os alunos se adaptam de forma muito receptível a esses métodos pelos mesmos estarem sempre buscando coisas novas. Assim a pesquisa trás uma forma interessante de se trabalhar o mesmo conteúdo dando um significado ao processo que antes era visto mecanicamente. Evidenciamos também que este é um trabalho de relevância para o ensino de Funções aonde foi visto atividades que contribuem pra o ensino dos alunos referentes aos conteúdos.

Pereira (2012) trouxe na sua dissertação um projeto que se objetivou em investigar o potencial didático da Criptografia e suas contribuições ao ensino de Matemática, tomando como ponto de partida os conhecimentos prévios dos alunos sobre Funções. A pesquisa teve duas turmas de Ensino Médio do Colégio Estadual Barão de Macaúbas, como cenário

investigativo, localizado no município de São Fidélis, interior do estado do Rio de Janeiro: uma turma de primeiro ano, com 21 alunos, e uma turma de segundo ano, com 20 alunos.

A metodologia desta pesquisa seguiu os referentes procedimentos primeiramente foram associados a atividades experimentais e indutivas aos alunos, que valorizam a análise e a descoberta, de forma a favorecer tanto a construção de conceitos matemáticos como o aprofundamento de conteúdos preexistentes envolvendo função, visando a facilitar o processo Ensino-Aprendizagem em Matemática.

A motivação desta dissertação surgiu em outubro de 2009, quando a pesquisadora supracitada acima lecionou em uma turma do primeiro ano do Ensino Médio de uma escola pública, para trabalhar com a disciplina Projetos, com carga horária de dois tempos semanais. A proposta consistia em reforços de conteúdo de Funções, tendo em vista a dificuldade dos alunos apresentando baixo rendimento, constatou de imediato a falta de interesse dos alunos que era evidente. Para eles, a disciplina Projetos resumia-se a resolver exercícios sobre Funções. Como estratégia para motivar a turma, a pesquisadora elaborou atividades envolvendo a Criptografia, nas quais os alunos, usando códigos e uma chave previamente combinada, trocavam mensagens entre si. Com isso, o interesse pelo assunto despertou e, “sem que eles percebessem”, estavam falando de associações, transformações, ou seja, sobre Funções.

No primeiro momento da intervenção com os alunos, foi favorecida a compreensão necessária do tema Criptografia e das relações codificar e decodificar. No segundo encontro, as atividades favoreciam discussões sobre Domínio e Imagem de Funções e Funções Inversíveis. Na turma chamada de 1002, pela pesquisadora, as chaves utilizadas representavam as Funções Afim e Quadrática. E as atividades eram postas de forma que favoreciam uma aprendizagem significativa, favorecendo o diálogo. Esta pesquisa teve um cunho qualitativo aonde buscava analisar os entendimentos do aluno com uma aprendizagem mais significativa. Em suma pode se constatar que o uso da Criptografia pode auxiliar no Ensino e Aprendizagem de tal conteúdo.

Segundo Pereira a aplicação das atividades usando a Criptografia como recurso, constatamos os três componentes descritos por Leontiev: necessidade, objeto e motivo – que são componentes estruturais da atividade. Os alunos tinham uma necessidade, que era decodificar a mensagem recebida; para satisfazer a essa necessidade, tinham de encontrar a função inversa – que é o objeto.

Desse modo, pode-se observar que os autores buscam uma nova perspectiva para o Ensino e Aprendizagem de Funções e Matrizes, tendo em vista um ensino motivador. As

metodologias mencionadas compreendem, basicamente, atividades que os alunos façam interligações dos conteúdos aprendidos em sala de aula com outros meios, sendo este a Criptografia que possui grandes contribuições ao se utilizar com a Matemática.

4 METODOLOGIA DA PESQUISA.

Esta pesquisa que privilegia a abordagem qualitativa busca investigar os problemas enfrentados pelos alunos e alunas, diante da aprendizagem do ensino de funções e matrizes no ensino médio. Segundo Oliveira (2007, p.37) a respeito de uma pesquisa qualitativa, o autor ressalta como sendo um processo de reflexão e análise da realidade através da utilização de métodos e técnicas para compreensão detalhada do objeto de estudo em seu contexto histórico e/ou sua estruturação.

De acordo com os PCN :

Falar de Ensino e Aprendizagem implica a compreensão de certas relações entre alguém que ensina, alguém que aprende e algo que é o objeto de estudo – no caso, o saber matemático. Nessa tríade, professor-aluno-saber, tem-se presente a subjetividade do professor e dos alunos, que em parte é condicionadora do processo de Ensino e Aprendizagem. (BRASIL, 2006, p.80).

Um ensino transmitido de uma forma interessante feito pelo professor reage de forma positiva para o aluno, aonde o mesmo interage em conjunto, conseguindo trabalhar com atividades que contribuam para o aperfeiçoamento da aprendizagem e do ensino.

Dessa maneira, a seguinte pesquisa se deu na Escola Cônego Fernando Passos, por ser uma instituição que está sempre disponível para intervenções didáticas. A instituição de ensino possui professores que buscam seu melhoramento profissional a cada dia, inovando a sua prática pedagógica a favorecimento dos alunos e da escola. Atualmente a escola está localizada na cidade de Passira-Pe. No panorama de obter dados, que estejam relacionados com a problemática da pesquisa, está sendo utilizada de forma qualitativa.

De acordo com Minayo (2007, p.174), a pesquisa qualitativa se caracteriza como uma “pesquisa de cunho compreensivo” e o ambiente estudado é o que se faz mais importante nessa perspectiva proporcionando ao pesquisador maior autonomia no processo de análise dos dados.

As transformações que ocorrem no ensino produtivo, que respeita as compreensões dos alunos e suas individualidades, são de suma importância para um processo de análise mais eficiente, respeitando o ambiente e os indivíduos que estão envolvidos nos processos investigativos.

A mesma foi realizada com uma turma de terceiro ano do ensino médio, a escolha da turma deu-se de forma espontânea pelo pensamento de que os alunos do terceiro ano do Ensino Médio possuíssem um raciocínio mais apurado sobre os conceitos e métodos matemáticos que seriam aplicados na pesquisa, dado que já teriam vistos os conteúdos anteriormente. Antes de realizar as intervenções na sala de aula sobre a pesquisa, informamos à coordenação da Escola, bem como ao professor titular da disciplina de Matemática, por meio de uma carta de apresentação, aonde esta esclarece todos os pontos referentes da pesquisa e mostra sua importância. (Apêndice1)

A pesquisa manifestou-se em investigar se os conhecimentos básicos que os alunos do Ensino Médio possuíam sobre o conteúdo de Funções e Matrizes pode ser potencializado diante de uma abordagem que incluía a Criptografia como estratégia didática.

Iniciando-se através de uma intervenção com os alunos revisando os conteúdos em conjunto com o professor da turma, com intuito de auxiliar os alunos a lembrarem os conteúdos e tirarem as dúvidas referentes às habilidades -possivelmente – “esquecidas” ou que em outro caso, “não teriam tido a oportunidade de estudar detalhadamente”. Dando espaço para que conseguissem absorver o conteúdo da melhor forma possível. Posteriormente foi explicada aos alunos a importância da pesquisa e foi lhes foi dada a oportunidade de escolha sobre a participação no trabalho. Os estudantes participantes assinaram um termo de consentimento livre e esclarecimento (TCLE) o qual explica um pouco da pesquisa e do tratamento de dados (Apêndice2). Assim participaram 16 alunos, os quais sabiam da responsabilidade de seus atos, e da importância da pesquisa.

Neste mesmo período foi aplicada uma atividade contendo perguntas abertas e questões relacionadas ao conteúdo propriamente dito. Essa atividade visou em observar a exposição dos conceitos matemáticos dos alunos em sala de aula e também as opiniões sobre os conteúdos, colocando quais eram as relevâncias e se os mesmos possuíam alguma aplicabilidade em outros contextos que não fossem na sala de aula, ainda sobre o teste também foi prestada atenção à forma da resolução dos alunos referente às questões que eles responderam sobre o conteúdo de funções e matrizes. (Apêndice 3).

Nesta etapa a prioridade foi analisar o discurso na resolução do aluno sobre os determinados conteúdos. Para a confecção deste trabalho foi consultado o livro integrado do Ensino Médio que a escola utiliza chamado Matemática Ciências e Aplicações, volume 3 do autor Gelson Iessi.

Na segunda etapa foi apresentada a Criptografia para os alunos, fazendo uma intervenção com a sala de aula explicando um pouco do contexto histórico com exemplos que

elucidaram o momento. Em seguinte foi mostrado aos alunos que a Criptografia pode ser aplicada a conteúdos matemáticos, a exemplo de Funções e Matrizes Para esta intervenção foi utilizado recurso de Datashow para facilitar ao máximo o entendimento do aluno sobre a aplicação da Criptografia no conteúdo matemático.

Nesta etapa foi aberto um momento para discursão do tema e tirar dúvidas dos alunos tanto sobre a Criptografia em si como as suas aplicações na matemática. Sem seguida, aplicamos uma atividade contendo questões abertas onde os alunos puderam escrever sobre os conceitos matemáticos relacionados à aplicação da Criptografia. Nesta questão os alunos puderam discorrer sobre o auxílio da aplicação para auxiliar o ensino de certos conteúdos matemáticos ou não, também nesta atividade houve questões sobre o conteúdo de Funções e Matrizes que utilizavam procedimentos criptográficos para resolução do mesmo (Apêndice 4). Nesta etapa também contivemos em analisar o discurso e as dificuldades na resolução do aluno sobre os determinados conteúdos. Para a elaboração deste questionário foi utilizada como referência alguns artigos que falam sobre o tema como Olgin (2011), Druck (2004), Tamarozzi (2003).

Compreendemos que pesquisar o processo de ensino e aprendizagem é essencial, pois, segundo Freire (1996), “não há ensino sem pesquisa e pesquisa sem ensino” (FREIRE, 1996, p.32). Tendo em vista este pensamento de Freire, vemos a necessidade de estar sempre pesquisando e desenvolvendo estudos que venham a contribuir com o ensino para os alunos.

Na terceira e última etapa foi feito uma análise dos resultados obtidos na turma, observando as possíveis contribuições que os alunos puderam transmitir através das atividades que responderam. Na atividade relacionada à questão aberta foi possível entender a compreensão dos alunos a respeito dos conceitos que os mesmos tinham e conseguiram absorver, pois puderam escrever sobre suas próprias opiniões sobre o tema, antes e depois do uso da criptografia. A respeito das questões que envolveram a utilização dos procedimentos matemáticos baseado no conceito de matrizes e funções, e posteriormente o uso da criptografia, conseguimos refletir sobre a importância de uma aplicação em relação com os resultados dos alunos por meio dos seus conhecimentos já adquiridos sobre o assunto e que puderam resolvê-los.

A análise será feita com base na Análise do Discurso de Norman Fairclough, ressaltando questões práticas e gerais da análise do discurso. Este estudo evidencia o discurso como prática social e não como fenômeno individual, o mesmo propõe que o discurso seja um modo de agir do indivíduo e suas representações. O discurso é visto com um olhar mais apurado buscando representações e significados para o indivíduo com o mundo, onde o

mesmo constrói e constituem suas identidades, relações, conhecimentos (FAIRCLOUGH, 2001).

Os discursos postos pelos indivíduos possibilitam uma significação no mundo, assim como seus processos, entidades e relações. Seguindo Fairclough, “O mesmo ocorre com o discurso como prática ideológica que constitui, naturaliza, mantém e transforma os significados do mundo de posições diversas nas relações de poder” (2001, p. 94).

Este estudo possui uma concepção tridimensional possuindo três categorias sendo elas:

1. O texto - Para o autor é visto como uma unidade constituída pela união entre significado e significante socialmente motivados, propagando a existência de razões sociais na relação de um fixo significante com um fixo significado.

Ao decidir utilizar a análise do texto, deveremos nos prender a quatro aspectos importantes sendo estes: O vocabulário, a gramática, a coesão e a estrutura textual.

2. A prática discursiva - Contém processos de produção, distribuição e consumo textual, possuindo alternâncias de acordo com seu contexto social. Os processos de produção e consumo podem ocorrer tanto individualmente como coletivamente. O mesmo pode ser distribuído de forma simples ou complexas de acordo com a escolha do pesquisador. Possuindo interpretações próprias levando em consideração o que os indivíduos possuem interiorizado. Este processo ocorre de maior ocorrência de forma inconsciente e mecânico.
3. A prática social - Parte da ideia que o discurso está envolto de ideologias baseadas na sociedade em que se encontram. Para isto Fairclough comenta:

as ideologias são significações/construções da realidade (o mundo físico, as relações sociais, as identidades sociais) que são construídas em várias dimensões das formas/sentidos das práticas discursivas e que contribuem para a produção, a reprodução ou a transformação das relações de dominação.(FAIRCLOUGH, 2001, p. 117).

Essas são relacionadas às práticas discursivas concretizando e caracterizando a fala dos indivíduos, que podem ser modificadas com o passar do tempo. O sujeito nesse caso pode possuir um posicionamento ideológico mais centrado, estabelecendo vínculos entre as práticas e as ideologias exigindo a mudança das práticas existentes.

Essas três dimensões podem ser explanadas de acordo com a especificidade da análise na qual o pesquisador se interessar para o seu trabalho. Para este utilizaremos a análise textual que é usada para se referir a qualquer material escrito ou falado. Realizando uma descrição

linguística do texto linguístico. A descrição consiste na identificação das estruturas do texto em termos de categorias descritivas, que podem assumir valor experiencial, relacional, expressivo, conetivo ou uma combinação destes. As estruturas estão ligadas a aspectos da prática social, como conteúdo, relações e sujeito, associados ao conhecimento, crenças, relações sociais, identidades sociais, entre outros (FAIRCLOUGH, 2001).

Nesse estudo foram respeitadas as Diretrizes e Normas Regulamentadoras das Pesquisas envolvendo Seres Humanos (Resolução 196/96-CNS/MS, 1996) através da garantia do sigilo quanto aos dados confidenciais da comunidade acadêmica envolvida na pesquisa, bem como o direito à liberdade de se recusar a participar ou de retirar o seu consentimento, em qualquer fase da pesquisa, sem penalização e sem prejuízo ao seu vínculo institucional.

5 ANÁLISE E RESULTADOS

Neste capítulo, serão apresentadas as análises por meio das coletas de dados obtidos através das atividades respondidas pelos discentes da escola estadual cônego Fernando Passos, os quais cursam o 3º ano do Ensino Médio. Em cada atividade, os alunos foram identificados da seguinte forma: *A1*, *A2*, até *A16* e para a segunda atividade foram identificados por *A'1*, *A'2* e assim sucessivamente até *A'16*.

A análise consiste em identificar através das atividades as contribuições da Criptografia no ensino de Funções e Matrizes, ou seja, se a introdução da aplicação da Criptografia enquanto estratégia didática leva o aluno a apurar seus conhecimentos em relação aos conteúdos supracitados acima. Esta análise utilizará a teoria de Norman Fairclough, explanado na metodologia, para tal serão observadas a produção textual, nas quais observaremos suas especificidades no decorrer da análise.

A análise dos dados dividiu-se em dois momentos. Uma análise descritiva da primeira e da segunda atividade, e posteriormente faremos uma análise comparativa entre a primeira e a segunda atividade observando as possíveis contribuições sobre este estudo.

5.1 ANÁLISE DESCRITIVA DA PRIMEIRA ATIVIDADE.

Neste momento foram agrupadas as respostas dos alunos em algumas categorias nas quais os sujeitos eram classificados conforme a resposta apresentada. As categorias foram: relação positiva sem especificação, relação de contribuição para os estudos, relação de contribuição para o âmbito social e relação negativa sem especificação, para cada categoria observamos certa conexão das respostas para fazer as inferências. Na primeira categoria encaixavam-se respostas que possuíam um cunho positivo em relação ao que se era perguntado, mais não possuía um desdobramento sobre o discurso, ou seja, não deixando muito claro a sua resposta. Já na segunda categoria eram observadas respostas que conduziam o discurso para o âmbito educacional e na terceira categoria era para o dia a dia, ou seja, utilização dos conteúdos fora da sala de aula, e na última categoria foram às respostas de negatividade ao que era perguntado.

Observemos a primeira questão:

- Qual a sua opinião sobre os conteúdos de Função e Matrizes em sala de aula? Por quê?

Cabia ao grupo de alunos se manifestarem sobre um direcionamento do que eles achavam sobre esses conteúdos trabalhados em sala, colocando suas opiniões de forma aberta. Para esta pergunta obtivemos as seguintes respostas:

Tabela 1: Mapeamento da primeira questão sobre a relação de contribuição conforme os entrevistados.

Relação positiva, sem especificação.	Relação de contribuição para os estudos	Relação de contribuição para o âmbito social	Relação negativa, sem especificação.
A 9: “Sim” A11: “Sim”	A1: “Bom, por que vamos precisar no futuro”. A2: “São conteúdos importantes, e que devem ser trabalhados em sala de aula”. A4: “Porque digamos que para dar continuidade há outros assuntos e de grande importância estuda-los com atenção para entender os seguintes”. A5: “É bom, porque não é tão difícil ao tanto de outros assuntos na Matemática”. A6: “É bom, pois é fácil e nos traz conhecimentos, sem contar que é ótimo para o raciocínio”. A7: “O conteúdo é bom, é um conteúdo fácil que auxilio no aprendizado básico da Matemática”. A10: “Os conteúdos de Função e Matrizes são ótimos, porque ajuda o aluno a desenvolver mais seu estímulo em Matemática”. A12: “São importantes, pois em várias avaliações necessita-se saber de Funções ou Matrizes”. A14: “É bom, porque nos ajuda e é fácil de entender”. A15: “Sim, porque é um assunto complexo de se entender”. A16: “Sim, porque busca todos os nossos conhecimentos. Matrizes é um conteúdo muito bom nós gostamos de assuntos”.	A3: “Acho que são conteúdos essenciais para o currículo estudantil, pois são conteúdos muito úteis em diversas ocasiões”. A8: “É importante além de ser um assunto simples e reutilizável fora da sala de aula”.	A13: “Não”.

Fonte: O autor, 2015.

Ao observar os discursos dos alunos A1, A2, A4, A5, A6, A7, A10, A12, A14, A15, A16 notamos que a maioria dos alunos teve um direcionamento das respostas em relação à contribuição nos estudos, tanto atual como vindouros, o que é de se esperar sendo estes alunos

do 3º ano do Ensino Médio. Em relação aos alunos A3 e A8, podemos ver que os mesmos relacionaram esta questão com utilidades do dia a dia, contribuindo no mundo fora da sala de aula, ou seja, o âmbito social. O aluno A13 fez referências negativas dos conteúdos explicitando sua dificuldade de entendimento, já os alunos A9 e A11, colocaram respostas positivas, porém não especificaram a sua relação, assim não conseguindo especificar de certo qual seria sua contribuição.

A segunda questão se deu da seguinte forma:

- Você considera o estudo de Funções e Matrizes importantes para a sua vida? Por quê?

Em relação a esta questão os alunos estavam deveriam a falar sobre a relevância dos conteúdos para sua vida, ou seja, se esses conteúdos teriam alguma contribuição para o seu dia a dia, se eles fossem importantes para se aprender em sala. Segue abaixo as respostas referentes a esta questão:

Tabela 2: Mapeamento da segunda questão sobre a relação de contribuição conforme os entrevistados.

Relação positiva, sem especificação.	Relação de contribuição para os estudos	Relação de contribuição para o âmbito social.	Relação negativa, sem especificação.

<p>A8: “Sim”.</p>	<p>A1: “Sim, por que é essencial para prestarmos vestibular e sabermos responder questões sobre esses assuntos”.</p> <p>A2: “Sim, em vestibulares, por exemplo, sempre há questões sobre esses assuntos”.</p> <p>A4: “Sim, para estimular os conhecimentos escolares”.</p> <p>A13: “Sim, porque se um dia eu for fazer uma faculdade que trabalhe muito com a matemática, já vou possuir um conhecimento prévio”.</p> <p>A15: “Sim, pois não só usamos esse conteúdo em sala de aula mais também em outras áreas da Matemática”.</p> <p>A16: “Para que futuramente eu possa ter mais conhecimento e mais aprendizagem sobre os conteúdos aprendidos em sala de aula”.</p>	<p>A3: “Sim, no dia-a-dia nos deparamos com situações que exigem o uso de funções e até mesmo de Matrizes”.</p> <p>A5: “Sim por que aprendemos mais e com certeza tudo que é aprendido de bom na nossa vida serve no futuro de cada um”.</p> <p>A6: “sim, pois podemos levar isso para fora no dia-a-dia”.</p> <p>A7: “Sim, porque pode ser utilizado em ações do dia-a-dia”.</p> <p>A9: “Sim, muito importante para calcular muitas coisas importantes no dia-a-dia”.</p> <p>A10: “Sim por que existem empregos que vão exigir saber de Funções e Matrizes no dia-a-dia do seu trabalho”.</p> <p>A11: “considero importante, pois mesmo que nós não percebemos usamos esses estudos no nosso dia-a-dia”.</p> <p>A12: “Sim, porque com essas e outras Funções aprendo novas coisas a cada dia”.</p> <p>A14: “Sim, por que para tudo que vamos fazer precisamos dela”.</p>	
-------------------	---	---	--

Fonte: O autor, 2015.

A partir dos discursos dos alunos A3, A5, A6, A7, A9, A10, A11, A12 A14 evidenciamos que a maioria deles escreveu sobre a relação de utilização dos conteúdos no dia a dia, fazendo relação a sua utilização fora da sala de aula, ou seja, foi encontrada no discurso dos alunos certa predominância da importância dos conteúdos para a vida social. Já para os alunos A1, A2, A4, A13, A15, A16, os conteúdos são vistos com bons olhos, porém a relação existente continua sendo relacionada com contribuições nos estudos, ou seja, os alunos fazem inferência a utilização dos conteúdos no âmbito escolar. E o aluno A8 discorre de forma positiva mais não apresentam um posicionamento sobre a relação de utilização dos conteúdos. Nesta questão 2 não foi encontrado no discurso dos alunos nenhuma relação de dificuldade e nenhuma relação negativa.

A terceira questão segue da seguinte maneira:

- Você acredita que estes conteúdos podem ser usados para outros fins, que não seja o da sala de aula?

Nesta pergunta, os alunos deveriam discorrer sobre a importância dos conteúdos no âmbito social com algumas aplicações que os mesmos poderiam vir a ter, especificando seus usos em outros contextos que não fossem o da sala de aula, observemos as respostas dos alunos referentes a esta questão:

Tabela 3: Mapeamento da terceira questão sobre a relação de contribuição conforme os entrevistados.

Relação positiva sem especificação	Relação de contribuição para os estudos	Relação de contribuição para o âmbito social	Relação negativa, sem especificação.
<i>A5: “Sim”.</i>	<p><i>A1: “Sim, por que quando nos tivemos um problema podemos jogar na Função e resolve-la”.</i></p> <p><i>A4: “Sim, pois um assunto é interligado a outro, desde o Ensino Fundamental ao Ensino Médio”.</i></p> <p><i>A6: “Sim, pois em uma Função o numero que atribuímos sempre vai dar um valor maior”.</i></p> <p><i>A7: “Sim, por exemplo, em funções se tivermos um valor inicial e utilizarmos ele em uma Função teremos outro valor distinto”.</i></p> <p><i>A9: “Sim, em alguns trabalhos por que a Matemática está em muitos deles”.</i></p> <p><i>A10: “Sim, por que a Matemática está envolvida com outras disciplinas”.</i></p> <p><i>A12: “Sim, em trabalhos profissionalmente necessita-se não só desses conteúdos mais de vários outros”.</i></p> <p><i>A14: “Sim, por que para entendermos engenharia precisamos saber um pouco</i></p>	<p><i>A2: “Sim, por que assim como todos os assuntos de Matemática, são utilizados no dia-a-dia, embora que em muitos casos usamos sem perceber”.</i></p> <p><i>A3: “Sim, realmente podemos usar Funções e Matrizes em nosso cotidiano em ocasiões nas quais as tentativas e erros são o caminho mais difícil”.</i></p> <p><i>A8: “Sim, podem ser usadas para muitas coisas, muitas que estão ao nosso redor”.</i></p> <p><i>A11: “Sim, por que a Matemática e tudo que estudamos nela são usadas no nosso cotidiano”.</i></p> <p><i>A13: “Sim, a esses conteúdos são essenciais em algumas profissões”.</i></p> <p><i>A16: “Sim, por que não devemos usar os nossos conhecimentos só em sala de aula mais também com</i></p>	

	<p><i>desses conteúdos”.</i></p> <p><i>A15: “Sim, com certeza, pois como disse na questão dois é usado em varias áreas Matemáticas”.</i></p>	<p><i>as pessoas por que assim podemos dialogar para aprendermos mais”.</i></p>	
--	--	---	--

Fonte: o autor, 2015.

O aluno A5, colocou discorreu positivamente, porém não especificou de forma clara a sua opinião, já os alunos A1, A4, A6, A7, A9, A10, A12, A14, A15 relacionaram suas respostas para os estudos, mesmo não sendo o objetivo da pergunta, pois a mesma se referia a ligação do conteúdos fora da sala de aula, porém os alunos não conseguiram fazer essa relação, mostraram que podia ser aplicado, mas ao discorrerem sobre a questão remeteram-se ao meio acadêmico novamente. Os alunos A2, A3, A8, A11, A13, A16 tiveram um discurso relacionado ao uso fora da sala de aula, como no cotidiano, no dia-a-dia, mas os mesmos não especificaram de fato a sua opinião, relacionando há alguma aplicação desse uso no cotidiano. Tendo em vista que eles possuem uma abrangência em relação ao uso da Matemática, porém não sabe ao certo onde e como podem ser usadas.

Observemos agora as questões que relacionam o conteúdo propriamente dito, ou seja, os conteúdos de Função Inversa, Matriz Inversa, Determinantes e Multiplicação de Matrizes. Para isto escolhemos duas atividades que irão representar as demais respostas dos alunos. Utilizaremos a atividade do aluno A1 para representar os alunos A2, A3, A5, A6, A7, A10 e A15 e o aluno A4 para representar os alunos A8, A9, A11 A12, A13, A14, A16. Para esta

separação foi observado as seguintes relações: o aluno que possuiu um bom desempenho respondendo todas as atividades sem nenhum erro procedimental, ficou encaixado na representação das questões do aluno *A1*, o aluno que acertou parcialmente as questões, ou deixou algumas em branco será representado pelas respostas do aluno *A4*.

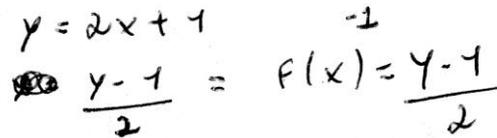
Para isto seguiremos a análise agora observando as respostas dos alunos supracitados acima em relação as questões 4 e 5. Observemos a seguir:

A quarta questão, tinha como objetivo observar se os alunos possuíam os conceitos sobre os conteúdos de função e função inversa, que fora explicado anteriormente no momento de intervenção. Observando se os erros dos alunos estavam relacionados a procedimentos básicos da Matemática, ou se os mesmos não tinham construído o conhecimento sobre o determinado assunto.

Observemos a resposta do aluno *A1* abaixo:

Figura 1: Resposta do aluno *A1* em relação à questão 4.a

4. Utilize os conceitos que você possui sobre funções e responda os seguintes itens:
a) Calcule a função inversa de $f(x) = 2x + 1$.



$$y = 2x + 1$$

$$\frac{y - 1}{2} = f(x) = \frac{y - 1}{2}$$

Fonte: O autor, 2015.

Podemos notar que o mesmo conseguiu realizar de forma correta os procedimentos chegando ao resultado desejado, já que a questão estava muito clara e os mesmos já tinham por meio da intervenção vista os procedimentos para a obtenção desses resultados.

Agora analisemos a mesma questão agora em relação ao aluno *A4*, para isso observemos a figura abaixo:

Figura 2: Resposta do aluno *A4* em relação à questão 4 .a

4. Utilize os conceitos que você possui sobre funções e responda os seguintes itens:
a) Calcule a função inversa de $f(x) = 2x + 1$.



$$f(x) = 2x + 1$$

$$\frac{y - 1}{2}$$

Fonte: O autor, 2015.

Para o aluno A4, notemos que ele conseguiu chegar ao resultado desejado, porém não fez o processo de forma detalhada evidenciando os passos a passos para obtenção dessa resposta.

Analisaremos agora a questão subsequente, ou seja, a letra b da questão 4. Observemos de início a resposta produzida pelo aluno A1.

Figura 3: Resposta do aluno A1 em relação à questão 4.b

b) Calcule os respectivos valores $f(1)$, $f(12)$, $f(23)$, $f(46)$, $f(123)$, para a função do item a, e repita o processo substituindo os valores que você encontrou na inversa da função.

$$f(x) = 2x + 1$$

$$f(1) = 2 \cdot 1 + 1 = 3$$

$$f(12) = 2 \cdot 12 + 1 = 25$$

$$f(23) = 2 \cdot 23 + 1 = 47$$

$$f(46) = 2 \cdot 46 + 1 = 93$$

$$f(123) = 2 \cdot 123 + 1 = 247$$

$\frac{y-1}{2} = x$
 $\frac{93-1}{2} = x \Rightarrow x = 46$
 $\frac{25-1}{2} = x \Rightarrow x = 12$
 $\frac{47-1}{2} = x \Rightarrow x = 23$
 $\frac{247-1}{2} = x \Rightarrow x = 123$

Fonte: O autor, 2015.

Nesta questão o aluno pode fazer as substituições de forma satisfatória, conseguindo resolver os procedimentos de forma correta chegando ao resultado desejado, ao observar de forma mais detalhada observamos que o mesmo possui algumas desordens na representação da resolução da questão, porém consegue-se identificar as respostas.

Seguiremos agora observando a resolução da questão 4, letra b) feita pelo aluno A4.

Figura 4: Resposta do aluno A4 em relação a questão 4.b

Calcule os respectivos valores $f(1)$, $f(12)$, $f(23)$, $f(46)$, $f(123)$, para a função do item a, e repita o processo substituindo os valores que você encontrou na inversa da função.

$$f(1) = 2 \cdot 1 + 1 = 2 + 1 = 3$$

$$f(12) = 2 \cdot 12 + 1 = 25$$

$$f(23) = 2 \cdot 23 + 1 = 47$$

$$f(46) = 2 \cdot 46 + 1 = 92$$

$$f(123) = 2 \cdot 123 + 1 = 246$$

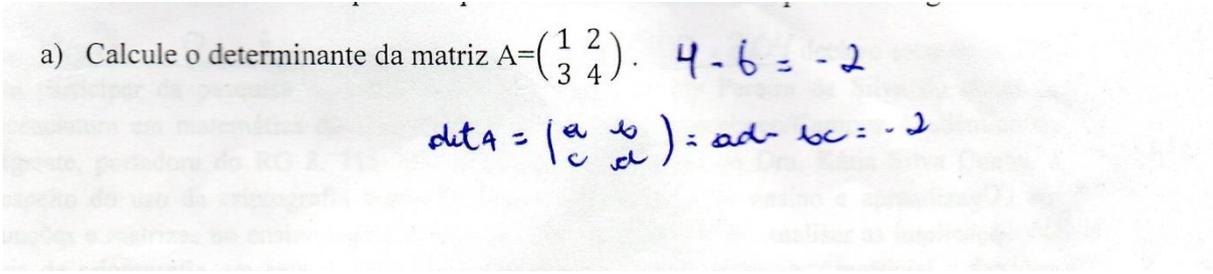
Fonte: o autor, 2015.

Para esta resolução observamos que o aluno efetua as substituições corretamente, porém não calcula os valores pedidos na Função Inversa, assim não executando todos os processos que foram pedidos na questão.

Seguiremos analisando a quinta questão que tem o objetivo de observar os erros presentes nas respostas dos alunos. Preocupando-nos em notar se os mesmos estavam relacionando os procedimentos básicos da Matemática de forma correta, ou se os mesmos não tinham construído o conhecimento sobre o determinado assunto, lembrando que o mesmo foi explicado e tirado dúvidas antes no momento de intervenção. Nesta questão o conteúdo especificado foi o de Matriz, onde podemos observar processos de Determinantes, Matriz Inversa e Multiplicação entre Matrizes.

Iniciando a análise da quinta questão, veremos a questão respondida pelo aluno *A1* na figura abaixo:

Figura 5: Resposta do aluno *A1* em relação a questão 5.a



a) Calcule o determinante da matriz $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. $4 - 6 = -2$

$$\det A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = -2$$

Fonte: O autor, 2015.

Notemos que o aluno *A1*, conseguiu construir o conhecimento sobre o cálculo de Determinantes e sua representação, expressou-se de forma clara, chegando ao resultado esperado. Tendo assim um bom desempenho na questão 5.a.

Para a mesma questão observaremos a resolução do aluno *A4*, notemos abaixo:

Figura 6: Resposta do aluno *A4* em relação a questão 5.a

a) Calcule o determinante da matriz $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

$$\det A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\det A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$$\det A = 4 - 6 = -2$$

Fonte: O autor, 2015.

O aluno A4, conseguiu responder corretamente esta questão, usando os procedimentos matemáticos visto no momento de intervenção de forma eficaz. Assim como todos os outros representados pelo aluno, alcançando assim o objetivo da questão.

Seguindo a análise veremos a letra b, desta mesma questão. Vejamos inicialmente a figura que representa a resposta do aluno A1:

Figura 7: Resposta do aluno A1 em relação à questão 5.b

b) Utilize a matriz do item anterior e calcule a sua inversa.

$$A^{-1} = \frac{1}{\det A} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{-2} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{4}{-2} & \frac{-2}{-2} \\ \frac{-3}{-2} & \frac{1}{-2} \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$$

Fonte: o autor, 2015.

Percebemos que o aluno A1, possui um bom desempenho na questão onde utiliza de forma correta os procedimentos matemáticos chegando assim ao resultado correto. Abaixo veremos a resposta do aluno A4, para essa mesma questão.

Figura 8: Resposta do aluno A4 em relação a questão 5.b

b) Utilize a matriz do item anterior e calcule a sua inversa.

$$A^{-1} = \frac{1}{\det A} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$A^{-1} = \frac{1}{-2} \begin{pmatrix} 1 & -2 \\ -3 & 4 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{-2} & -1 \\ \frac{1}{-2} & -2 \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{-2} \cdot -2 = \frac{-2}{-2} \\ \frac{1}{-2} \cdot -3 = \frac{-3}{-2} \\ \frac{1}{-2} \cdot 4 = \frac{4}{-2} \end{pmatrix}$$

Fonte: o autor, 2015.

O aluno A4, nesta resolução cometeu alguns erros relacionados à substituição dos valores da Matriz, não substituindo-a corretamente, assim efetuou as operações individualmente não colocando os valores da Matriz corretamente, porém se montarmos a Matriz da forma com que o aluno estava pensando ainda ocasionaria um erro pelo fato da troca no momento de substituição inicialmente. Também observamos nesta resolução que o aluno identifica quais procedimentos tem que ser feito, mas ainda não possui uma relação estreita com a representação correta da Matriz, assim não chegando ao resultado desejado.

Por fim observamos a letra c da quinta questão, encerrando assim as questões presentes na primeira atividade. Veremos primeiramente a resposta do aluno A1:

Figura 9: Resposta do aluno A1 em relação a questão 5.c

c) Faça a multiplicação de matrizes utilizando a matriz A e sua inversa.

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} -2+3 & 1+(-1) \\ -6+6 & 3-2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Fonte: O autor, 2015.

Notamos que o aluno *A1*, respondeu de forma eficiente o que a questão pediu conseguindo chegar ao resultado desejado. É notório a eficácia do aluno em relação ao conteúdo, conseguindo seguir todos os procedimentos de forma correta sem ocasionar nenhum erro. Para esta mesma questão, observaremos novamente a resposta do aluno *A4*.

Figura 10: Resposta do aluno *A4* em relação a questão 5.c.

c) Faça a multiplicação de matrizes utilizando a matriz *A* e sua inversa.

$$A \cdot A^{-1} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

Fonte: O autor, 2015.

Por fim notemos que o aluno *A4*, iniciou a representação do que seria feito na questão, porém não chegou a concluí-la, deixando a questão sem a resposta final, os alunos que o aluno *A4* representou também apresentaram esse mesmo descaso com esta questão, não concluindo sua resolução.

Assim a primeira análise referente à primeira atividade proporcionou uma boa interação no que diz respeito tanto a opinião dos alunos como seus conhecimentos mais específicos da área Matemática. Podendo notar que os alunos em sua maioria acreditam que a Matemática pode ser introduzida no dia-a-dia, mesmo que por muitas vezes relacionem-na com a vida acadêmica e não com um contexto realmente fora da sala de aula. Os alunos colocam que os conteúdos são de suma importância para a sua vida, mas acontece que alguns desses que dispõem desse discurso não possuem uma construção positiva sobre os conteúdos, possuindo ainda muita dificuldade em relação a sua resolução. De forma ampla podemos perceber que os alunos conseguem visualizar a Matemática com um olhar mais afetivo, sabendo de sua necessidade para a vida e para carreira seja ela escolar ou profissional. Em relação às questões que requeriam a resolução dos alunos podemos ver que a sala ficou dividida, ou seja, metade dos alunos conseguiu resolver o que foi pedido nas questões, e outra metade apresentou certa dificuldade, não resolvendo que se era solicitado.

5.2 ANÁLISE DESCRITIVA DA SEGUNDA ATIVIDADE.

Neste momento de análise seguiremos o mesmo raciocínio utilizado na análise da primeira questão. Porém, agora tomaremos atenção na relação com o uso da criptografia ao conteúdo, ou seja, as possíveis contribuições que a criptografia pode oferecer aos alunos e suas relações ao uso desta aplicação na sala de aula com os conteúdos de função e matrizes. Assim as categorizações irão ser especificadas a esta linha de raciocínio sendo dispostas da seguinte forma: relação positiva sem especificação, relação de contentamento com o uso da criptografia, relação de descontentamento com uso da criptografia e relação negativa. Nesta categoria podemos observar que a relação positiva sem especificação e relação negativa é utilizada na primeira análise e terão o mesmo uso e as mesmas explicações na sua classificação, já a relação de contentamento e descontentamento com o uso da criptografia foi introduzida para esta análise tendo em vista a necessidade de observar este discurso nas falas dos alunos. Para essas relações serão observadas as respostas que fazem referências positivas com especificações a respeito da pergunta, notando minuciosamente a resposta do aluno e a relacionando com essas categorias.

Observemos a primeira questão da segunda atividade:

- Você considera que a utilização da Criptografia como aplicação ao ensino de Funções e Matrizes pode facilitar no entendimento dos conteúdos? Por quê?

Nesta pergunta, cabia aos alunos expressarem suas opiniões sobre o uso da Criptografia como facilitador no processo de ensino, ou seja, se a utilização desta aplicação pode ajudar na compreensão do conteúdo de uma forma mais simples e motivadora fazendo com que os alunos tenham mais incentivos e motivação para responder as atividades que lhe são propostas. Verifiquemos as respostas dos alunos na tabela abaixo:

Tabela 4: Mapeamento da primeira questão sobre a relação de contentamento conforme os entrevistados.

Relação positiva sem especificação	Relação de contentamento com o uso da criptografia	Relação descontentamento com o uso da criptografia	Relação negativa sem especificação.
---	---	---	--

<p>A'5: "Sim". A'6: "Sim".</p>	<p>A'1: ". "Sim, porque é uma forma simples de se resolver Funções Matrizes". A'2: "Sim, pois muitos alunos poderão achar mais fácil para a aprendizagem". A'3: "Sim, porque é bem pratico e interessante." A'4: "Sim, pois tem uma forma mais comunicativa, desenvolvendo as atividades de forma menos cansativa". A'7: "Sim, porque é fácil de entender e de fazer os procedimentos". A'10: "Sim, porque é outra forma de aplicar nossos conhecimentos sobre os conteúdos". A'12: "Sim, porque se tem uma capacidade melhor de se compreender sobre o conteúdo". A'15: "Sim, porque acabou sendo um jeito simples e pratico de se fazer tendo outra forma".</p>	<p>A'8: "Não, pois fica mais complexo para entender". A'9: "Não, porque a Criptografia e mais complicada porque envolve um modo de codificação". A'11: "Não, porque fica mais complicado". A'14: "Não, pois fica mais complexo".</p>	<p>A'13: "Não". A'16: "Não".</p>
------------------------------------	---	--	--------------------------------------

Fonte: o autor, 2015.

Observemos que a maioria dos alunos obtiveram posicionamentos satisfatórios sobre o uso da Criptografia, onde podemos evidenciar através dos discursos dos alunos A'1, A'2, A'3, A'4, A'7, A'10, A'12 e A'15. Os alunos A'5 e A'6 relacionaram positivamente o uso da Criptografia para os conteúdos, porém não deram nenhuma justificativa sobre o seu direcionamento. Já os alunos A'8, A'9, A'11 e A'14, formaram opiniões de desagrado colocando que o uso da Criptografia pode dificultar o processo de aprendizagem dos conteúdos, ou seja, ficando mais complexos, e os alunos A'13 e A'16 colocaram que a criptografia não pode auxiliar no entendimento dos conteúdos, mas não especificaram suas respostas, assim não podendo obter um entendimento mais detalhado sobre o motivo das suas opiniões. Seguiremos com a análise da segunda questão da segunda atividade.

- O sua concepção sobre Funções e Matrizes continua o mesmo de antes, quando você não sabia desta relação do conteúdo? Por quê?

Esta questão tinha como objetivo observar se o uso da Criptografia contribuiu em relação ao conceito dos conteúdos, se a mesma pode ajudar os alunos a visualizar de forma mais ampla os conteúdos fazendo com que os alunos expandissem seus limites sobre o conteúdo construindo novas relações com o que era visto antes. Observe as respostas dos alunos sobre essa questão:

Tabela 5: Mapeamento da segunda questão sobre a relação de contribuição conforme os entrevistados.

Relação positiva sem especificação.	Relação de contentamento com o uso da criptografia	Relação descontentamento com o uso da criptografia	Relação negativa sem especificação
	<p>A'1: “Não, porque agora usamos a Criptografia para escrever mensagens codificando e decodificando”.</p> <p>A'2: “Não, pois tem muito mais coisas do que eu imaginava e sabia, e com o uso da Criptografia pude aprender”.</p> <p>A'3: “Não, achava que Matrizes e Funções se limitavam apenas aos exercícios”.</p> <p>A'4: “Não, pois agora os conteúdos foram vistos de forma mais organizada e interessante”.</p> <p>A'6: “Não, agora aprendi que os conteúdos podem ser usados para varias coisas”.</p> <p>A'7: “Não, porque a Criptografia mostrou outro lado de se utilizar Matrizes e Funções”.</p> <p>A'10: “Não, depois que teve essa explicação posso entender o que eu nem sabia que existia sobre Funções e Matrizes”.</p> <p>A'14: “Não, porque quando não sabia dessa utilidade, não imaginava para que podia ser usado esses conteúdos e com a explicação ficou fácil de fazer”.</p> <p>A'15: “Não, ficou mais fácil de entender”.</p>	<p>A'5: “Sim, pois não gostei dessa utilização”.</p> <p>A'8: “Sim, pois continuo usando o modo anterior”.</p> <p>A'9: “Sim, porque continuo usando os mesmos conceitos”.</p> <p>A'11: “Sim, pois continua as mesmas operações”.</p> <p>A'12: “Sim, pois continuo usando o que usava antes”.</p> <p>A'13: “Sim, porque eu não achei interessante”.</p> <p>A'16: “Sim, porque continuamos utilizando sempre as mesmas coisas”.</p>	

Fonte: O autor, 2015.

Em relação a esta pergunta não tivemos nenhuma resposta sem justificativa, todos tentaram expressar suas opiniões sobre as possíveis mudanças que a Criptografia poderia ocasionar para o ensino, nove dos alunos, sendo eles A'1, A'2, A'3, A'4, A'6, A'7, A'10, A'14 e A'15 discorreram positivamente evidenciando o uso da Criptografia como um agente eficaz, que relaciona os conteúdos de forma mais simples levando-os a um melhor desempenho educacional, ou seja, auxiliando num melhoramento dos conceitos dos conteúdos, Já os demais A'5, A'8, A'9, A'11, A'12, A'13, A'16 colocaram que o uso da Criptografia recai no uso dos mesmos processos matemáticos, assim não mudando o conceito que eles já possuem sobre o conteúdo, ainda o A'5 e o A'13 discorreram contra o uso da Criptografia, colocando que não era interessante, que não tinham gostado.

Evidenciamos a quinta questão, que possui o seguinte enunciado:

- Depois de ter o contato com a Criptografia relacionada aos conteúdos de Função e Matriz, você considera que estes conteúdos são importantes para a sua aprendizagem? E para o âmbito social? Por quê?

Nesta questão cabiam os alunos, escrever sobre a importância dos conteúdos em vista a utilização deles em uma aplicação que fora visto anteriormente, se a mesma pode contribuir dando importância ao que se é estudada em sala levando os conteúdos para um campo mais amplo de conhecimento para os alunos.

Para visualizar veremos as respostas dos alunos sobre essa pergunta na tabela abaixo:

Tabela 6: Mapeamento da terceira questão sobre a relação de contribuição conforme os entrevistados.

Relação positiva sem especificação	Relação de contentamento com o uso da criptografia	Relação descontentamento com o uso da criptografia	Relação negativa, sem especificação.

	<p>A'1: <i>“Sim, porque conseguimos usar os conteúdos que aprendemos em algo fora da sala de aula”.</i></p> <p>A'2: <i>“Sim, porque conseguimos visualizar melhor os conteúdos com algo do cotidiano”.</i></p> <p>A'3: <i>“Sim, ajuda-me a compreender o que significam os conteúdos e aplica-los a codificação”.</i></p> <p>A'4: <i>“Sim, pois podemos observar que o que aprendemos é usado fora da sala de aula de uma forma interessante”.</i></p> <p>A'5: <i>“não, pois não fez diferença na minha aprendizagem”.</i></p> <p>A'6: <i>“Sim, pois auxilia na compreensão de que a Matemática está presente em tudo na nossa volta”.</i></p> <p>A'7: <i>“Sim, porque podemos compreender algumas formas em que a Matemática está presente”.</i></p> <p>A'8: <i>“Sim ,pois construí um novo olhar sobre a Matemática”.</i></p> <p>A'9: <i>“Sim, porque é uma maneira simples e fácil de se visualizar a Matemática no cotidiano”.</i></p> <p>A'10: <i>“Sim, porque a Criptografia se utiliza da Matemática para ajudar no processo de codificação e decodificação”.</i></p> <p>A'11: <i>“Sim, pois pude notar uma aplicação fácil e interessante sobre a Matemática”.</i></p> <p>A'12: <i>“Sim, pois aprendemos a Matemática pura na sala e aplicamos na Criptografia”.</i></p> <p>A'14: <i>“Sim, pois se entendermos a Matemática podemos aplica-la a muitas coisas como na Criptografia”.</i></p> <p>A'15: <i>“Sim, pois a Matemática é importante ela pode ser aplicada a muitas coisas como na Criptografia”.</i></p>	<p>A'13: <i>“Não, pois eu não irei utilizar esses conteúdos de nenhuma forma”.</i></p>	<p>A'16: <i>“ Não”.</i></p>
--	--	--	-----------------------------

Fonte: O autor, 2015.

Nestas respostas podemos visualizar que a maioria dos alunos discorreram receptíveis ao uso da Criptografia, ressaltando a importância dos conteúdos para a sua aprendizagem e em relação ao uso fora da sala de aula, conseguindo estabelecer uma relação da Matemática com sua aplicação, expandindo o seu uso além das dimensões escolar, conseguindo enxergar a sua aplicabilidade os alunos que obtiveram esses raciocínios foram A'1, A'2, A'3, A'4, A'5, A'6, A'7, A'8, A'9, A'10, A'11, A'12, A'14 e A'15. Já o aluno A'13 não foi receptível, expressando uma insatisfação sobre o uso desta aplicação nos conteúdos, explicitando que não

vai contribuir na sua aprendizagem e A'16 mostrou uma relação negativa, mas não expõe sua opinião sobre o assunto.

Verifiquemos agora as questões que utilizaram a Criptografia como aplicação nos conteúdos de Função e Matrizes. Neste momento de análise escolhemos duas atividades que irão representar as demais respostas dos alunos. Utilizaremos a atividade do aluno A'10 para representar os alunos A'1, A'2, A'3, A'4, A'5, A'6, A'7 e A'15 e o aluno A'9 para representar os alunos A'8, A'11, A'12, A'13, A'14, A'16. Para esta seleção observamos as seguintes relações: o aluno que demonstraram um bom desempenho respondendo todas as atividades não apresentando erros seja procedimental ou conceitual, ficou encaixado na representação das questões do aluno A'10, o aluno que acertou parcialmente as questões, ou deixou algumas em branco será representado pelas respostas do aluno A'9.

Para isto seguiremos a análise observando as respostas dos alunos supracitados acima em relação à primeira e segunda questão desta atividade.

A primeira questão foi a seguinte:

- Utilize os conceitos que você possui sobre Funções aplicada a Criptografia e responda a questão seguindo os procedimentos criptográficos.

Nesta questão o aluno seria induzido a utilizar os conteúdos matemáticos que tinham visto na atividade anterior fazendo inferência a Criptografia, no uso da codificação e decodificação da mensagem dada na questão. Observe a figura abaixo:

Figura 11: Resposta do aluno A'10 em relação a questão 1

- a) Utilize a função $f(x) = 3x + 2$, para codificar a seguinte mensagem "AULA ANIMADA" e a inversa da função $f(x)$ para decodificar.

Handwritten work showing the encoding and decoding of the message "AULA ANIMADA" using the function $f(x) = 3x + 2$.

Message: AULA ANIMADA
 Encoded: 1 21 12 1 11 4 9 13 1 4 1

Function: $f(x) = 3x + 2$
 Inverse: $f(x) = \frac{x-2}{3}$

Calculations for encoding:

- $f(1) = 3 \cdot 1 + 2 = 5$
- $f(21) = 3 \cdot 21 + 2 = 65$
- $f(12) = 3 \cdot 12 + 2 = 38$
- $f(1) = 3 \cdot 1 + 2 = 5$
- $f(11) = 3 \cdot 11 + 2 = 35$
- $f(4) = 3 \cdot 4 + 2 = 14$
- $f(9) = 3 \cdot 9 + 2 = 29$
- $f(13) = 3 \cdot 13 + 2 = 41$
- $f(1) = 3 \cdot 1 + 2 = 5$
- $f(4) = 3 \cdot 4 + 2 = 14$
- $f(1) = 3 \cdot 1 + 2 = 5$

Calculations for decoding:

- $f(x) = \frac{5-2}{3} = \frac{3}{3} = 1$ A
- $f(x) = \frac{65-2}{3} = \frac{63}{3} = 21$ U
- $f(x) = \frac{38-2}{3} = \frac{36}{3} = 12$ L
- $f(x) = \frac{5-2}{3} = \frac{3}{3} = 1$ A
- $f(x) = \frac{35-2}{3} = \frac{33}{3} = 11$ I
- $f(x) = \frac{14-2}{3} = \frac{12}{3} = 4$ N
- $f(x) = \frac{29-2}{3} = \frac{27}{3} = 9$ I
- $f(x) = \frac{41-2}{3} = \frac{39}{3} = 13$ M
- $f(x) = \frac{5-2}{3} = \frac{3}{3} = 1$ A
- $f(x) = \frac{14-2}{3} = \frac{12}{3} = 4$ N
- $f(x) = \frac{5-2}{3} = \frac{3}{3} = 1$ A

A segunda questão desta atividade envolvia a Criptografia com o uso de Matrizes, onde o aluno necessitaria fazer as operações que tinham visto no momento de intervenção anteriormente. Nesta questão observamos de forma análoga os mesmos pontos para classificação. Esta possui o seguinte enunciado:

- Utilize os conceitos que você possui sobre Matrizes aplicada a Criptografia e responda a questão abaixo:

Observemos a resposta do aluno A'10.

Figura 13: Resposta do aluno A'10 em relação a questão 2

Utilize a matriz $B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ para codificar a mensagem "ENSINO MÉDIO" e a inversa da matriz B para decodificar a mensagem original.

$$B = \begin{pmatrix} 5 & 14 & 19 & 9 & 14 & 15 \\ 13 & 5 & 4 & 9 & 15 & 0 \end{pmatrix} \cdot A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 & 14 & 19 & 9 & 14 & 15 \\ 13 & 5 & 4 & 9 & 15 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 40+13 & 28+5 & 38+4 & 18+9 & 28+15 & 30+0 \\ 5+13 & 14+5 & 19+4 & 9+9 & 14+15 & 15+0 \end{pmatrix}$$

$$\begin{pmatrix} 23 & 33 & 42 & 27 & 43 & 30 \\ 18 & 19 & 23 & 18 & 29 & 15 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 23 & 33 & 42 & 27 & 43 & 30 \\ 18 & 19 & 23 & 18 & 29 & 15 \end{pmatrix}$$

$$\begin{pmatrix} 23-18 & 33-19 & 42-23 & 27-18 & 43-29 & 30-15 \\ -23+25 & -33+38 & -42+45 & -27+35 & -43+38 & -30+30 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 14 & 19 & 9 & 14 & 15 \\ 13 & 5 & 4 & 9 & 15 & 0 \end{pmatrix}$$

Fonte: O autor, 2015.

Nesta resolução o aluno A'10, utilizou-se dos procedimentos matemáticos corretamente chegando ao resultado desejado, ou seja, codificando e decodificando a mensagem. O aluno

conseguiu realizar de forma correta e objetiva em relação aos procedimentos obtendo êxito na resolução.

Veremos a seguir a figura que representa a mesma questão sendo respondida pelo aluno A'9. Observe abaixo:

Figura 14: Resposta do aluno A'9 em relação a questão 2.

Utilize a matriz $B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ para codificar a mensagem “ENSINO MÉDIO” e a inversa da matriz B para decodificar a mensagem original.

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 & 14 & 19 & 9 & 14 & 15 \\ 13 & 5 & 4 & 9 & 15 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 10 & 28 & 38 & 18 & 28 & 30 \\ 26 & 10 & 8 & 18 & 30 & 0 \end{pmatrix}$$

Fonte: o autor, 2015.

Nesta questão respondida pelo aluno A'9, podemos evidenciar que o aluno não conseguiu fazer as operações corretas, tendo dificuldade na operação de Multiplicação de Matrizes, errando os valores dessa operação e o mesmo não terminou o processo de codificação e decodificação da mensagem, não completando o objetivo da questão.

Ao terminar a análise desta segunda atividade, constatamos que os alunos em sua maioria tiveram uma boa impressão do uso da Criptografia relacionada com Funções e Matrizes, acreditando que ela pode levar o aluno a ter uma aprendizagem mais fácil e prazerosa, complementando que a mesma pode dar significado ao estudo destes conteúdos em sala. Em relação à mudança das relações sobre o conteúdo, os alunos ficaram quase divididos, acreditando que a Criptografia pode contribuir para a construção de um conhecimento mais aprimorado e os demais alegou que este uso não faz nenhuma diferença em relação o estudo destes conteúdos. Em relação às questões de codificar e decodificar pode-se notar que mais da

metade dos alunos conseguiram resolver de forma satisfatória, ou seja, conseguiram entender os procedimentos e aplica-los de forma correta, alcançando o objetivo da questão.

5.3 ANÁLISE COMPARATIVA ENTRE A PRIMEIRA E SEGUNDA ATIVIDADE.

Neste momento nos prenderemos a discutir as principais informações que conseguimos abstrair das atividades que os alunos responderam, colocando pontos de suma importância para a pesquisa como: houve contribuições no uso da Criptografia em relação aos conteúdos para os alunos? A mesma viabilizou uma utilização significativa par o Ensino e Aprendizagem? e ainda a Criptografia obteve resultados motivadores para relação da importância dos conteúdo?

Através das respostas dos alunos na primeira atividade, podemos observar que a maioria relacionava os conteúdos apenas com o âmbito escolar, não sendo utilizados de forma pratica na sociedade. Ainda sobre a primeira atividade é claro notar que os alunos ao serem perguntados da importância dos conteúdos para sua vida, tentaram responder sobre sua utilidade no dia a dia, mas nenhum conseguiu exemplificar esse uso cotidiano, deixando claro que os mesmos não identificaram nenhuma maneira de utilização desses conteúdos no âmbito social, ou seja, por muitas vezes os alunos escreviam da utilidade dos conteúdos fora da sala de aula, mas não sabiam como e nem aonde aplica-los. Porém na segunda atividade podemos notar que os alunos conseguem claramente discursar sobre o uso dos conteúdos na Criptografia para codificação e decodificação, assim já possuindo uma utilidade para o uso dos conteúdos fora do âmbito escolar.

Ainda em relação à segunda atividade podemos notar que os alunos entenderam o objetivo da aplicação, considerando que a maioria dos alunos respondeu que a Criptografia pode vim a facilitar no entendimento dos alunos a respeito dos conteúdos e ainda que a Criptografia torna o ensino dos conteúdos mais importantes dando assim significado ao que se é estudado em sala.

Em relação às questões ligadas aos conteúdos propriamente ditos podemos notar que houve uma alteração positiva, onde antes apenas metade dos alunos tinha efetuado a resolução de todas as questões de forma correta outros tinham obtidos erros e deixados questões sem fazer. Com o uso da Criptografia mais da metade, ou seja, 10 alunos conseguiram resolver as

questões de codificação e decodificação, obtendo êxito na construção do conhecimento desta aplicação.

Todavia, os alunos que não obtiveram êxito nas questões utilizando Criptografia foram os mesmos que tiveram dificuldade na resolução das questões na primeira atividade, retirando dois alunos que antes cometeram erros e com o uso da Criptografia conseguiram superar. Assim podemos notar que a Criptografia é um meio de ajudar reforçar e até contribuir para a compreensão do assunto para os alunos que já possuem certo conhecimento, ou seja, tendo uma certa apropriação dos conteúdos. Para os alunos que não possuem um conhecimento mais aprimorado dos conteúdos a Criptografia não consegue facilitar na sua aprendizagem, ocasionando certo desagrado pela aplicação, pois os mesmos que não conseguiram resolver a atividade de codificação e decodificação discorreram negativamente sobre o uso da Criptografia comentando que seu uso deixa os conteúdos mais complexos, entre outros comentários.

Entretanto, mesmos os alunos que não tiveram um bom desempenho com o uso da Criptografia e com sua relação com a Matemática, consideraram em sua maioria que após ter visto a Criptografia aplicada aos conteúdos, os mesmos tornaram-se mais importantes tanto para o sua aprendizagem como para sua vida, dando sentido e significado ao que se é estudado em sala.

Então ao nos deparar com esses dados podemos constatar que o uso da Criptografia em um modo geral contribuiu positivamente em relação aos conteúdos para os alunos. Pode proporcionar uma interação ao que antes se via apenas ligado ao âmbito escolar para o âmbito social, criando ligações significativas na construção do saber, fazendo com que os alunos em sua maioria se sintam motivados a responder questões sobre Funções e Matriz.

CONSIDERAÇÕES FINAIS

Ao finalizarmos esta pesquisa acadêmica, podemos observar a importância do uso de Criptografia para o ensino de Matemática, onde os alunos puderam relacionar e refletir sobre os conteúdos estudados em sala de aula. Esta pesquisa conseguiu extrair dos alunos discursos muito interessantes sobre o uso da Criptografia aplicada aos conteúdos de Função e Matrizes. Os alunos em sua maioria foram receptivos a esta aplicação alegando a sua importância aos conteúdos.

De acordo com Meirelles (2011), atividades que envolvem criptografia contribuem significativamente para desenvolvimento dos conhecimentos ligados a operações com matrizes, estimulando uma forma motivadora de buscar o aprimoramento do conhecimento. De fato, podemos observar que os alunos se sentiram mais auspiciosos em resolver as atividades com o uso da criptografia tanto nos momentos em que se utilizavam matrizes, como também nos procedimentos que envolviam funções.

Com este estudo também evidenciamos que para a utilização eficaz desta aplicação os alunos devem ter um conhecimento prévio e maduro dos conteúdos utilizados. Conforme a pesquisa de Rodrigues (2013):

As atividades com a criptografia tornam a aula mais interessante e dessa forma chama mais a atenção do aluno instigando-o a investigar, questionar e procurar soluções. Porém deve se levar em conta duas variáveis.

- 1) Os alunos devem possuir um conhecimento sobre o conteúdo a ser trabalhado por meio da criptografia.
- 2) É necessário saber o grau de conhecimento que o aluno traz consigo sobre o conhecimento trabalhado. (p. 34).

Percebemos que ao termino do nosso trabalho conseguimos responder todas as nossas indagações colocadas no inicio da pesquisa, em que através das respostas dos alunos nas atividades conseguimos visualizar as implicações que a criptografia pode ocasionar aos alunos. Essas implicações foram em sua grande maioria positivas, o uso da criptografia pode corroborar com a ampliação da mentalidade dos alunos em relação aos conteúdos, lhes dando uma amplitude da relação da Matemática com o cotidiano.

Diante desses fatos, acreditamos que a utilização da Criptografia relacionada aos conteúdos do Ensino Médio pode contribuir ao ensino e aprendizagem dos alunos de maneira

interessante e eficaz, porém sabendo-se das especificidades de cada aluno, de modo que a criptografia atinge com maior proporção os alunos que já possuem certa habilidade Matemática, ou seja, os alunos que possuem dificuldades nos procedimentos matemáticos não conseguem atingir o processo de codificação e decodificação, mas pode proporcionar curiosidade e estímulo para que possam relacionar a Matemática com o cotidiano, dando sentido e significado ao que se é estudado em sala de aula.

Outras pesquisas vindouras utilizando a criptografia relacionada ao Ensino Médio pode ser vista utilizando os mesmos conceitos em relação a outros conteúdos Matemáticos que os alunos vêm e que por muitas vezes são vistos de formas superficiais e até mesmo sem ligação com o dia-a-dia como a Aplicar o Princípio Fundamental da Contagem, Combinação Simples e Números de Subconjuntos. Evidenciando também os discursos dos professores em relação a esta forma de aplicação dos conteúdos, discutindo a importância e a viabilidade de se trabalhar em sala de aula com os alunos, assim tendo uma gama de informações tanto dos alunos como dos professores em relação à Criptografia sendo utilizada aos conteúdos do Ensino Médio.

REFERÊNCIAS BIBLIOGRÁFICAS

- BRASIL, Ministério da Educação. Secretaria de Educação Ensino Médio. PCN (**Parâmetros Curriculares Nacionais para o Ensino Médio - PCNEM**); Parte III. Brasília: SEF/MEC, 1999.
- BRASIL, Ministério da Educação. Secretaria de Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais (Ensino Médio)**. Brasília: MEC, 2000.
- BRASIL, Secretaria de Educação Ensino Médio. (**Orientações Curriculares para o Ensino Médio- OCEM**). Brasília: MEC/SEB, 2006.
- BRASIL, Ministério da Educação. Secretaria da Educação Básica. **PCN + (Orientações Educacionais Complementares aos Parâmetros Curriculares Nacionais – Ensino Médio)**; Brasília: SEF/MEC, 2002.
- CANTORAL, R. et al. (2003). Desarrollo del pensamiento matemático. México, Trillas: ITESM, UniversidadeVirtual.
- COUTINHO, S. **Números inteiros e Criptografia RSA**. Sociedade Brasileira de Matemática, 2000.
- DANTE, L. R. Matemática: Contextos e aplicações- volume único; 3.ed. 2009.
- DRUCK, S. & HELLMEISTER, CATARINA, A. P. & PEIXOTO, MONTEIRO, C. **Coleção Explorando o ensino- Matemática-** vol 3. Brasília: Ministério da educação, Secretaria de educação básica, 2004.
- FAIRCLOUGH, N. **Discurso e mudança social**. Editora UnB. Brasília, 1992/2001.
- FERREIRA, S. R. I. **Aplicações de Matrizes no Ensino Médio**. Disponível em www.teses.usp.br/teses/disponiveis/55/55136/.../DisSilviaRevisada.pdf>. Acesso em 26 de junho de 2015.
- FIARRESGA, V. M. C. **Criptografia e Matemática**. Disponível em < http://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf>. Acesso em 16 de maio de 2015.
- FINCATTI, C. Á. **Criptografia como agente motivador na aprendizagem da Matemática em sala de aula**. Disponível em< http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-24362007000100005>. Acesso em 29 de maio de 2015.
- FRANÇA, W. B. A. **A utilização da Criptografia para uma aprendizagem contextualizada e significativa**. Disponível em: < http://bit.profmatsbm.org.br/xmlui/bitstream/handle/123456789/1336/2012_01132_WALDIZAR_BORGES_D_E_ARAUJO_FRANCA.pdf?sequence=1>. Acesso em 05 de agosto de 2015.
- FREIRE, P. Pedagogia da Autonomia: Saberes necessários à Prática Educativa. São Paulo: Paz e Terra, 1996.
- GODINHO, D. S.; CESARIO, G. L.; REIS, J. N.; SARAIVA, R. S. **“CRIPTOGRAFIA”:** A Importância da Álgebra Linear para Decifrá-la. Disponível em

<http://www.facos.edu.br/old/galeria/130072011050939.pdf>>. Acesso em 20 de agosto de 2015.

GROENWALD, C. L. O.; OLGIN, C. A. Criptografia e o Currículo de Matemática no Ensino Médio. **Revista de Educação Matemática: Sociedade Brasileira de Educação Matemática**, São Paulo, v. 13, n. 15, p. 69 – 78, 2011.

GROENWALD, C. L. O.; NUNES, G. S. **Currículo de Matemática no ensino básico: a importância do desenvolvimento dos pensamentos de alto nível**. Disponível em <http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-24362007000100005>. Acesso em 28 de junho de 2025

JESUS, A. L. N. **Criptografia na educação básica: Utilização da Criptografia como elemento motivador para o Ensino Aprendizagem de Matrizes**. Disponível em <http://bit.profmatsbm.org.br/xmlui/bitstream/handle/123456789/872/2011_00649_ANDRE_LUIS_NERIS_DE_JESUS.pdf?sequence=1>. Acesso em 18 de agosto de 2015.

KUERTEN, C. **Algumas aplicações de Matrizes**. Disponível em <https://repositorio.ufsc.br/bitstream/handle/123456789/96804/Cristini_Kuerten.PDF?sequence=1>. Acesso em 19 de agosto de 2015.

LITOLDO, B. F. **As Potencialidades de Atividades Envolvendo Problemas de Criptografia na Construção do Conteúdo de Função Afim**. disponível em <www.lematec.no-ip.org/CDS/XVIIIIBRAPEM/PDFs/GD3/litoldo3.pdf>. Acesso em 5 de agosto de 2015.

LOURENÇO, F. O. **Tópicos de Criptografia para o Ensino Médio**. Disponível em <http://bit.profmatsbm.org.br/xmlui/bitstream/handle/123456789/1528/2012_01339_FLAVIO_ORNELLAS_LOUREIRO.pdf?sequence=1>. Acesso em 10 de agosto de 2015.

MARQUES, T. V. **Criptografia: abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula**. Disponível em <http://bit.profmatsbm.org.br/xmlui/bitstream/handle/123456789/281/2011_00133_THIAGO VALENTIM M ARQUES.pdf?sequence=1>. Acesso em 15 de maio de 2015.

MEIRELES, M. M. **A Criptografia como Elemento Motivador para o Ensino das Operações Matriciais**. Disponível em <<https://sites.google.com/a/unemat-net.br/sietcon/trabalho-de-conclusao-de-curso/tcc-2011-2/tcc-moises-martins-meireles>>. Acesso em 05 de agosto de 2015.

MINAYO, M. C. de S. **O Desafio do Conhecimento: pesquisa qualitativa em saúde**. 10 Ed., São Paulo, Hucitec, 2007.

MEIRELES, M. M. **A Criptografia como Elemento Motivador para o Ensino das Operações Matriciais**. Disponível em <<https://sites.google.com/a/unemat-net.br/sietcon/trabalho-de-conclusao-de-curso/tcc-2011-2/tcc-moises-martins-meireles>>. Acessado em 05 de agosto de 2015.

MENEZES, S. **Mensagens secretas com Matrizes – Criptografia**. Disponível em: <www.ime.unicamp.br/.../AtividadeFinal_Criptografia28092013.pdf>. Acesso em 22 de junho de 2015.

NIETO, S. dos S.; LOPES, C. M. C.; SILVA, A. F. **Criptografia: Uma aplicação de Álgebra Linear.** Disponível em <http://www.mackenzie.br/fileadmin/Graduacao/EE/Producao/2008intertechcriptografia_1_.pdf>. Acesso em 7 de agosto de 2015.

OLIVEIRA, D.; KRIPKA, R. M. L. **O uso da Criptografia no ensino da Matemática.** In: Conferência Internacional de Educação Matemática, XIII, 2001. Disponível em <<http://webcache.googleusercontent.com/search?q=cache:55MoQrCVVfKJ:www.gente.eti.br/lematec/CDS/XIIICIAEM/artigos/1817.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br>>. Acesso em 25 de outubro de 2015.

OLIVEIRA, M.M: **Como fazer uma pesquisa qualitativa.** Petrópolis, Rio de Janeiro: Ed. Vozes, 2007.

PEREIRA, V. da S. S. **Ensino de Funções: uma abordagem contextualizada do Tratamento da informação no Ensino Médio.** Disponível em <<http://www.uss.br/arquivos;jsessionid=878FE3484470177F9A43419B1A7EA8C0/posgraduacao/strictosensu/educacaoMatematica/dissertacoes/2012/VIVIANE.pdf>>. Acesso em 14 de setembro de 2015.

RODRIGUES, J. de M.. **Criptografia e conteúdos de Matemática no Ensino Fundamental.** Disponível em <<http://bit.profmatsbm.org.br/xmlui/handle/123456789/840>>. Acesso em 10 de agosto de 2015.

SANTOS, J. L. **A arte de cifrar, criptografar, esconder e salvaguardar como fontes, motivadoras para atividades de Matemática básica.** Disponível em <http://bit.profmatsbm.org.br/xmlui/bitstream/handle/123456789/208/2011_00046_JOSE_LUIZ_DOS_SANTOS.pdf?sequence=1>. Acesso em 20 de agosto de 2015.

SILVA, A. A. **Números, Relações e Criptografia.** Departamento de Matemática – UFPB, Paraíba, 2000.

SINGH, S. **O livro dos Códigos.** Record, 2001. Disponível em: <<http://pt.slideshare.net/IgorRibeiro1/63942184primeirocapitolodolivradoscodigossimonsingh>>. Acesso em 29 junho 2015.

SHOKRANIAN, S. **Criptografia para Iniciantes.** Brasília: UnB, 2005.

TAMAROZZI, A. C. **Codificando e decifrando mensagens.** Disponível em <www.educadores.diaadia.pr.gov.br/arquivos/File/...de.../RPM45_08.PDF>. Acesso em 22 de junho de 2015.

TERADA, R. Criptografia e a importância das suas aplicações. **Revista do Professor de Matemática (RPM).** No 12, 1º semestre de 1988.



APÊNDICE 1
CARTA DE APRESENTAÇÃO



De: Prof^ª Dra. Kátia silva Cunha (Prof^ª Adjunta do NFD/CAA/UFPE)

À: Coordenação da Escola de Ensino Médio cônego Fernando Passos.

Assunto: Solicitação de autorização para realização de Pesquisa Acadêmica.

Vimos, por meio desta, apresentar uma proposta de realização de Pesquisa intitulada: **“O USO DA CRIPTOGRAFIA COMO FACILITADOR DO PROCESSO DE ENSINO E APRENDIZAGEM EM FUNÇÕES E MATRIZES NO ENSINO MÉDIO”** a ser desenvolvida sob a coordenação da Profa. Dra. Kátia Silva Cunha.

A citada pesquisa será desenvolvida pela aluna Paula Mirely Pereira da Silva (nº de matrícula: 099.322.194-79) regularmente matriculada no Curso de Licenciatura em Matemática da Universidade Federal de Pernambuco (UFPE), no Centro Acadêmico do Agreste (CAA).

Por acreditarmos na relevância do tema, necessitamos da colaboração da referida escola para que a nossa pesquisa seja viabilizada e, futuramente, seus dados possam contribuir para a melhoria do processo de ensino e aprendizagem.

Ressaltamos que as informações obtidas a partir deste estudo serão rigorosamente confidenciais. Os resultados serão divulgados publicamente, entretanto, a identidade da escola e dos participantes jamais será revelada. Não haverá qualquer tipo de custo por parte das escolas, nem dos participantes, sendo a colaboração totalmente voluntária.

Ficamos no aguardo da respectiva autorização e agradecemos de antemão, renovando os nossos votos de respeito e consideração.

Atenciosamente,

Assinatura da orientadora

Assinatura da pesquisadora

Caruaru, _____ de _____ de 2015.



APÊNDICE 2



TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Pesquisa: O USO DE CRIPTOGRAFIA COMO FACILITADOR DO PROCESSO DE ENSINO E APRENDIZAGEM EM FUNÇÕES E MATRIZES NO ENSINO MÉDIO.

Pesquisadora: Paula Mirely Pereira da Silva (tel.:(81)999026827 email:paulamirelypereira@hotmail.com)

Orientadora: Kátia Silva Cunha (tel.: 988741574 e-mail: kscunha@gmail.com)

Eu _____ RG _____ declaro estar de acordo em participar da pesquisa realizada pela aluna Paula Mirely Pereira da Silva do curso de licenciatura em Matemática da Universidade Federal de Pernambuco/Campus Acadêmico do Agreste, portadora do RG 8. 715 717, orientada pela professora Dra. Kátia Silva Cunha, a respeito do uso da Criptografia como facilitador do processo de Ensino e Aprendizagem em Funções e Matrizes no Ensino Médio pesquisa , que se propõe em analisar as implicações do uso da Criptografia em sala de aula, com respeito ao estudo de Álgebra Matricial e Funções. Fazendo com que tanto o professor quanto os alunos consigam visualizar a importância da aplicação para um ensino motivador. Estou ciente de que as respostas serão para a pesquisa, podendo aparecer em possíveis publicações. Fica garantida minha liberdade de desistência de participar da pesquisa a qualquer momento, bem como o sigilo e o anonimato, sem que ocorra qualquer tipo de coerção ou prejuízo. Fica garantida minha liberdade de não responder a questões que me causem algum constrangimento. Quanto a custos e receita, estas são nulas, não havendo qualquer tipo de despesa de minha parte, ou ganho com minha participação nesta pesquisa. Recebi todas as informações necessárias, estando ciente dos objetivos dessa pesquisa. Serão mantidos todos os preceitos éticos legais durante e após o término da pesquisa. O termo de consentimento livre e esclarecido autoriza a utilização dos dados pelos integrantes da referida equipe de pesquisa e que tal autorização é uma pré-condição bioética para execução de qualquer estudo envolvendo seres humanos sob qualquer forma ou dimensão, em consonância com a resolução 196/96 do Conselho Nacional de Saúde. Este termo será realizado em duas vias para que uma fique com o entrevistado e outra com a pesquisadora. Em caso de dúvida, poderei entrar em contato com a pesquisadora pelos endereços ou telefones citados acima. Cientes dos termos propostos, concordo em participar da pesquisa.

Caruaru, _____ de _____ de 2015.

Assinatura do participante

Assinatura da pesquisadora



APÊNDICE 3

Universidade Federal de Pernambuco

Núcleo de Formação Docente

Centro Acadêmico do Agreste

Curso de Matemática-Licenciatura

Orientadora: Kátia Silva Cunha

Coorientadora: Maria Do Desterro A. da Silva

Discente: Paula Mirely Pereira da Silva

Pesquisa sobre O Uso da Criptografia no Processo de Ensino e Aprendizagem em Funções e Matrizes no Ensino Médio

Aluno _____

Atividade

- Qual a sua opinião sobre os conteúdos de função ou matrizes em sala de aula? Por quê? _____

- Você considera o estudo de funções e matrizes importante para sua vida? Por quê? _____

- Você acredita que estes conteúdos podem ser usados para outros fins, que não seja o da sala de aula? Por quê? _____

4. Utilize os conceitos que você possui sobre funções e responda os seguintes itens:
- Calcule a função inversa de $f(x) = 2x + 1$.
 - Calcule os respectivos valores $f(1)$, $f(12)$, $f(23)$, $f(46)$, $f(123)$, para a função do item a, e repita o processo substituindo os valores que você encontrou na inversa da função.
5. Utilize os conceitos que você possui sobre matrizes e responda os seguintes itens:
- Calcule o determinante da matriz $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$
 - Utilize a matriz do item anterior e calcule a sua inversa.
 - Faça a multiplicação de matrizes utilizando a matriz A e sua inversa.



APÊNDICE 4



Universidade Federal de Pernambuco

Núcleo de Formação Docente

Centro Acadêmico do Agreste

Curso de Matemática-Licenciatura

Orientadora: Kátia Silva Cunha

Coorientadora: Maria Do Desterro A. da Silva

Discente: Paula Mirely Pereira da Silva

Pesquisa sobre O Uso da Criptografia no Processo de Ensino e Aprendizagem em Funções e Matrizes no Ensino Médio

Aluno _____

Atividade

A tabela de codificação e decodificação abaixo, será utilizada nas questões 1 e 2 a seguir:

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	26

1. Utilize os conceitos que você possui sobre funções aplicada a criptografia e responda a questão seguindo os procedimentos criptográficos.

Utilize a função $f(x) = 3x + 2$, para codificar a seguinte mensagem “AULA ANIMADA” e a inversa da função $f(x)$ para decodificar.

2. Utilize os conceitos que você possui sobre matrizes aplicada a criptografia e responda a questão abaixo:

Utilize a matriz $B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ para codificar a mensagem “ENSINO MÉDIO” e a inversa da matriz B para decodificar a mensagem original.

3. Você considera que a utilização da criptografia como aplicação ao ensino de funções e matrizes pode facilitar no entendimento dos conteúdos? Por quê? _____

4. O seu conceito sobre funções e matrizes continua o mesmo de antes, quando você não sabia desta relação do conteúdo? Por quê? _____

5. Depois de ter o contato com a criptografia relacionada aos conteúdos de função e matriz, você considera que estes conteúdos são importantes para a sua aprendizagem? E para o âmbito social? Por quê? _____
