SOCIEDADE BRASILEIRA DE MATEMÁTICA
FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

RAILEI GARCIA LEAL

CRIPTOGRAFIA NA SALA DE AULA: UMA APLICAÇÃO DA TEORIA DAS FUNÇÕES E MATRIZES.

PORTO VELHO
2016

RAILEI GARCIA LEAL

CRIPTOGRAFIA NA SALA DE AULA: UMA APLICAÇÃO DA TEORIA DAS FUNÇÕES E MATRIZES.

Trabalho de conclusão apresentado ao Mestrado Profissional em Matemática em Rede Nacional – PROFMAT no Polo da Fundação Universidade Federal de Rondônia – UNIR, como requisito parcial para obtenção do título de Mestre, sob a orientação do Prof. Dr. Marinaldo Felipe da Silva.

PORTO VELHO

2016

FICHA CATALOGRÁFICA
BIBLIOTECA PROF. ROBERTO DUARTE PIRES

Leal, Railei Garcia.

L435c

Criptografia na sala de aula: Uma aplicação da teoria das funções e das matrizes. / Railei Garcia Leal, Porto Velho, 2016.

48f.; il.

Orientador: Prof. Dr. Marinaldo Felipe da Silva

Dissertação (Mestrado em Matemática) – Fundação Universidade Federal de Rondônia, Porto Velho, 2016.

1. Criptografia. 2. Funções. 3 Matrizes. I. Fundação Universidade Federal de Rondônia. II. Título.

CDU: 517.5:37

Bibliotecário responsável: Luã Silva Mendonça- CRB11/905

RAILEI GARCIA LEAL

CRIPTOGRAFIA NA SALA DE AULA: UMA APLICAÇÃO DA TEORIA DAS FUNÇÕES E MATRIZES

Este Trabalho foi julgado e aprovado para a obtenção do título de Mestre em Matemática Profissional no Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional da Sociedade Brasileira de Matemática, Polo da Universidade Federal de Rondônia.

Porto Velho, 25 de novembro de 2016.

Prof. Dr. Marinaldo Felipe da Silva
Coordenador no Polo da Universidade Federal de Rondônia do Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UNIR

COMISSÃO EXAMINADORA

Prof. Dr. Marinaldo Felipe da Silva
Orientador/Presidente
PROFMAT/UNIR

Prof.ª Ms. Marizete Nink de Carvalho
Membro Interno
PROFMAT/UNIR

Prof.ª Drª. Maria das Graças V. de Souza
Membro Externo
UNIR

“A matemática é o alfabeto com o qual
DEUS escreveu o universo”

Pitágoras

Dedico esta dissertação à minha família que sempre esteve presente e me apoia em todos os meus projetos. Em especial aos meus pais, e a minha filha que é minha maior fonte de inspiração.

AGRADECIMENTOS

Agradeço primeiramente a DEUS, por sempre ter iluminado minha vida e meus caminhos, e ter me ajudado a chegar no fim de mais essa jornada.

Ao Prof. Marinaldo pela paciência, pela orientação, e por ter acreditado em mim. E aos demais professores do Mestrado, em especial, os professores: Adeilton, Thomás, Ronaldo e Flávio.

À professora e amiga Maria das Graças por ser uma fonte inspiradora em como ensinar e amar a matemática.

Aos meus pais e meus irmãos (Raiden e Railene), por serem pessoas especiais em minha vida, e grandes incentivadores.

A minha filha por sempre me contagiar com sua alegria constante, e me ensinar a sorrir sempre mesmo quando choramos.

A minha esposa Aline Leal, pelos incentivos que sempre recebo, por ser tão especial em minha vida e por estar ao meu lado juntamente com minha filha nessa reta final.

Aos meus amigos que participaram dessa jornada juntamente comigo e me ajudaram, em especial a amiga Samantha, pelas ajudas durante todo o curso e pela grande amizade.

Aos meus amigos de trabalho da Politec de Tangará da Serra pelas várias permutas de plantões, permitindo assim que eu participasse das aulas.

Ao diretor da Escola Estadual 29 de Novembro por ter autorizado a realização da oficina, e a professora de Matemática Josimara por ter fornecido seu tempo e algumas de suas turmas para que a oficina de matemática tivesse êxito.

E a todos que de alguma forma, fizeram e fazem parte da minha vida.

Muito obridado!

RESUMO

Neste trabalho, mostraremos um relato histórico da criptografia e seus conceitos, e abordaremos alguns tópicos de funções e matrizes, com conceitos, definições e propriedades, mostrando logo em seguida aplicações desses conteúdos com a criptografia que podem ser aplicados em sala de aula, e na parte final mostrar o trabalho realizado na Escola Estadual 29 de Novembro com algumas atividades proposta aplicadas e que relacionam o conteúdo abordado durante o ano e a criptografia com os alunos do Ensino Médio.

Palavras chave: Criptografia. Funções. Matrizes.

ABSTRAT

This work shows a historical account of cryptography and concepts, and discusses some topics of functions and matrices, with concepts, definitions and properties, then showing content applications with an encryption that can be applied in the classroom, and in Part Final show the work carried out at the State School 29 de Novembro with some activities applied and that relate the content addressed during the year and the cryptography with the students of the High School.

Key word: Encryption. Functions. Arrays.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

O pouco tempo que trabalhamos em sala de aula, serviu de muito aprendizado tanto com os alunos quanto com os colegas docentes, a forma de transmitir, explicar um certo conteúdo, muita das vezes se tornava algo desafiador.

> *'O papel do professor é mediar e não ensinar. Ao aluno, por sua vez, cabe a construção do seu conhecimento por meio do esforço pessoal' (Beltrameem, 2015).*

E é justamente esse desafio, essa paixão, que faz com que o título "Como encantar o aluno", de onde foi retirada a citação anterior, torne-se algo crucial para este trabalho.

A matemática do ensino fundamental e médio, dependendo do "Mediador", pode ser muito estimulante para o aluno, foi justamente pensando nisso, que realizamos pesquisas de determinados temas, como o raciocínio lógico, funções e matrizes, buscando formas de criar nos alunos essa busca por mais conhecimento.

Algo que serve de estímulo é sempre você ver de forma simples uma aplicação do que está sendo visto em sala de aula, principalmente quando essa aplicação é algo que esteja sendo usado diariamente mesmo sem o aluno saber, que é o caso da CRIPTOGRAFIA, algo que está constantemente no noticiário.

Durante o 10º Encontro Nacional de Educação Matemática realizado na Bahia, em 2010, houve a apresentação do trabalho: Criptografia na sala de aula, realizado por Luiza de Abreu Menezes e Marcos Pavani de Carvalho, que tinha como objetivo principal a melhoria da qualidade do ensino da Matemática nos diversos níveis.

É evidente que a criptografia é algo muito abrangente que envolve conteúdos que vão desde números primos, passando por decomposição, álgebra até chegarmos em teoria dos números, porém esse não é o objetivo, queremos aqui mostrar de forma simples através de uma linguagem um pouco mais informal para que os alunos venham entender o princípio dela e verificar aplicações de conteúdos como função e matrizes de forma dinâmica, para que posteriormente sirva de "curiosidade" para busca de novos horizontes.

Sendo assim o objetivo geral deste trabalho é descrever uma breve introdução da criptografia, além de fornecer ao Professor de matemática ferramentas para uma aplicação em sala de aula, afim de tornar as aulas mais dinâmicas, para que assim aja uma busca maior pelo conhecimento por parte dos alunos.

Os objetivos específicos são:

- Introduzir e relatar fatos históricos da Criptografia;
- Relacionar a criptografia com funções e matrizes;
- Apresentar problemas relacionados com funções e matrizes.
- E estimular o raciocínio dos alunos através de mecanismos mais dinâmicos trabalhados em sala de aula.

Na primeira seção, mostraremos um breve relato histórico da criptografia, focando principalmente na cifra de substituição.

Na segunda seção, faremos uma introdução de funções, definições, função inversa, e focando em seguida nas lineares.

Na terceira seção, faremos um estudo resumido do conteúdo de matrizes, mostrando suas operações, além de definições importantes como matrizes inversíveis.

Na sequência, na quarta seção, mostraremos o trabalho que foi realizado durante uma semana com algumas turmas do ensino médio da Escola Estadual 29 de Novembro, mostrando as atividades que foram aplicadas, tanto relacionadas a função, quanto a matrizes, aplicadas a criptografia.

1 CRIPTOGRAFIA

Nesta seção abordaremos o conceito de criptografia, fazendo um breve relato histórico da criptografia, destacando fatos importantes como o telegrama de Zimmermann, além da criptografia de substituição.

1.1 O QUE É CRIPTOGRAFIA?

Desde que se iniciou o processo por parte dos homens, no envio de mensagens, tem havido a necessidade de protege-las de curiosos. E é justamente isso que é a Criptografia (em grego: *kryptós*, "escondido", e *gráphein*, "escrita") é um meio de transformação de texto simples para texto cifrado, através de um mecanismo que chamamos de chave secreta.

1.2 HISTÓRIA DA CRIPTOGRAFIA

Acredita-se que a criptografia teve seu início por volta de 2000 a.C no Egito, hieróglifos eram usados nos túmulos de reis e governantes, os quais contavam muita das vezes relatos importantes de suas vidas.

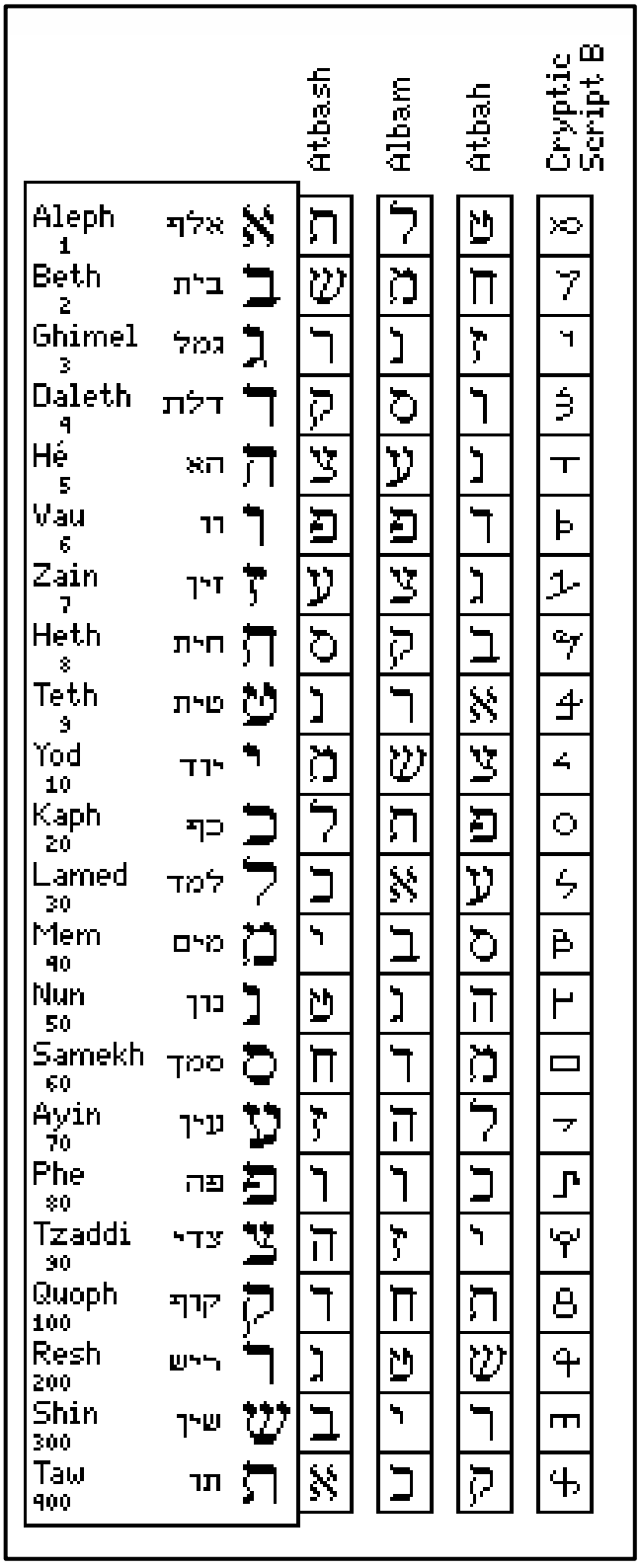
Um relato que chega a ser engraçado é que pela criptografia ser algo misterioso para a maioria das pessoas, imaginavam que havia a ligação com algum ritual de magia negra, fazendo com que os primeiros estudiosos da criptografia fossem vistos como seguidores do diabo.

Na Mesopotâmia e na Babilônia eram usados técnicas similares ao Egito. Já na Bíblia era muita das vezes usado uma codificação Hebraica, que consistia na permutação das letras do alfabeto, a última se torna a primeira, a penúltima se torna a segunda e assim por diante, ou seja, a palavra MATEMÁTICA era escrita no código NZGVNZGRXZ, essa criptografia Hebraica era conhecida como *Atbash*, ainda tinha o *Albam* e o *Atbah*.

Temos também uma técnica moderna da cifra de substituição que tem seu primeiro registro de uso feita por Júlio César, a técnica consistia em substituir as letras no texto por uma que é três posições para a direita, ou seja, o ‘A’ torna-se ‘D’, a ‘B’

torna-se ‘E’ e assim por diante. Nunca ninguém soube o motivo de ser atribuído estas três posições.

Figura 1 – Alfabeto e os sistemas de codificação Hebraico

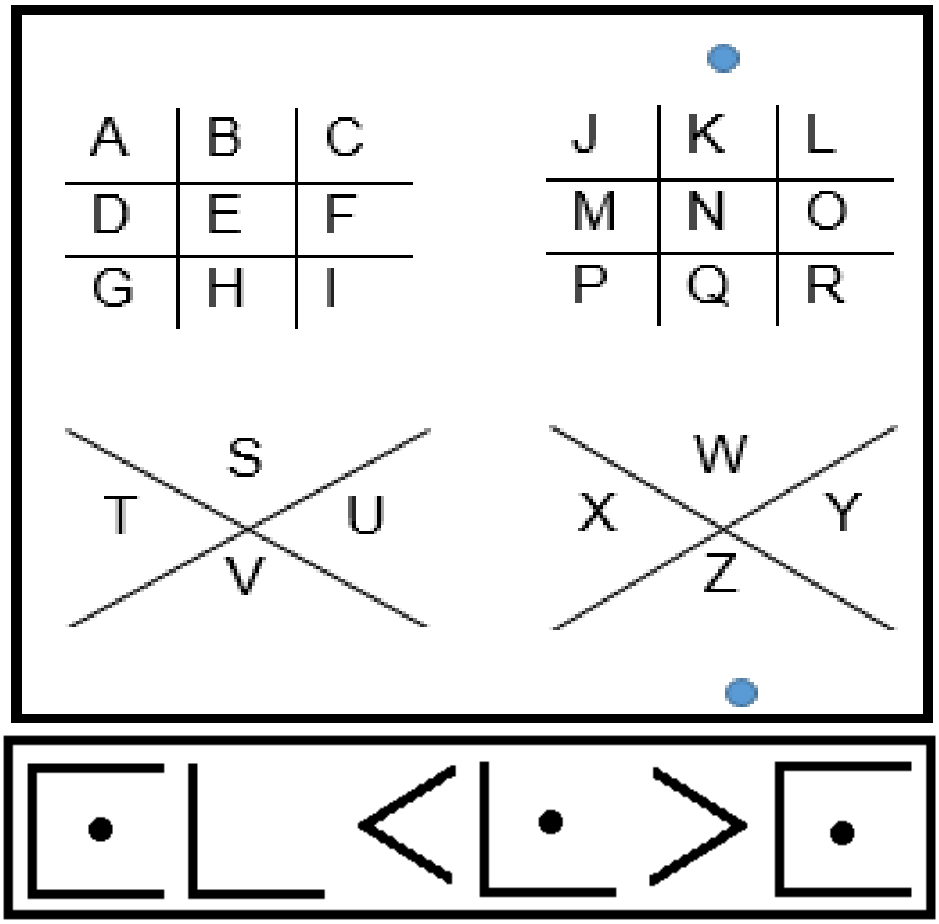


Disponível em: http://www.numaboa.com.br/criptografia/124-substituicao-simples/168-atbash. Acesso em: 14 out 2016

E por último temos também o alfabeto maçônico que surgiu na França por volta de 1745, sendo divulgado no catecismo francês da maçonaria por Louis Travenol, alfabeto este herdado na realidade dos tempos antigos, descobertos pelos árabes no século oitavo, e desenvolvido e organizado pelos cabalistas judeus, e adaptados por ocultistas e hermetistas cristãos ao longo da Idade Média e do Renascimento.

No século XVIII, ele era muito usado por cultivar o gosto pelo oculto e o secreto, conforme ilustrado na figura 2.

Figura 2 – Alfabeto maçônico e palavra OCULTO.



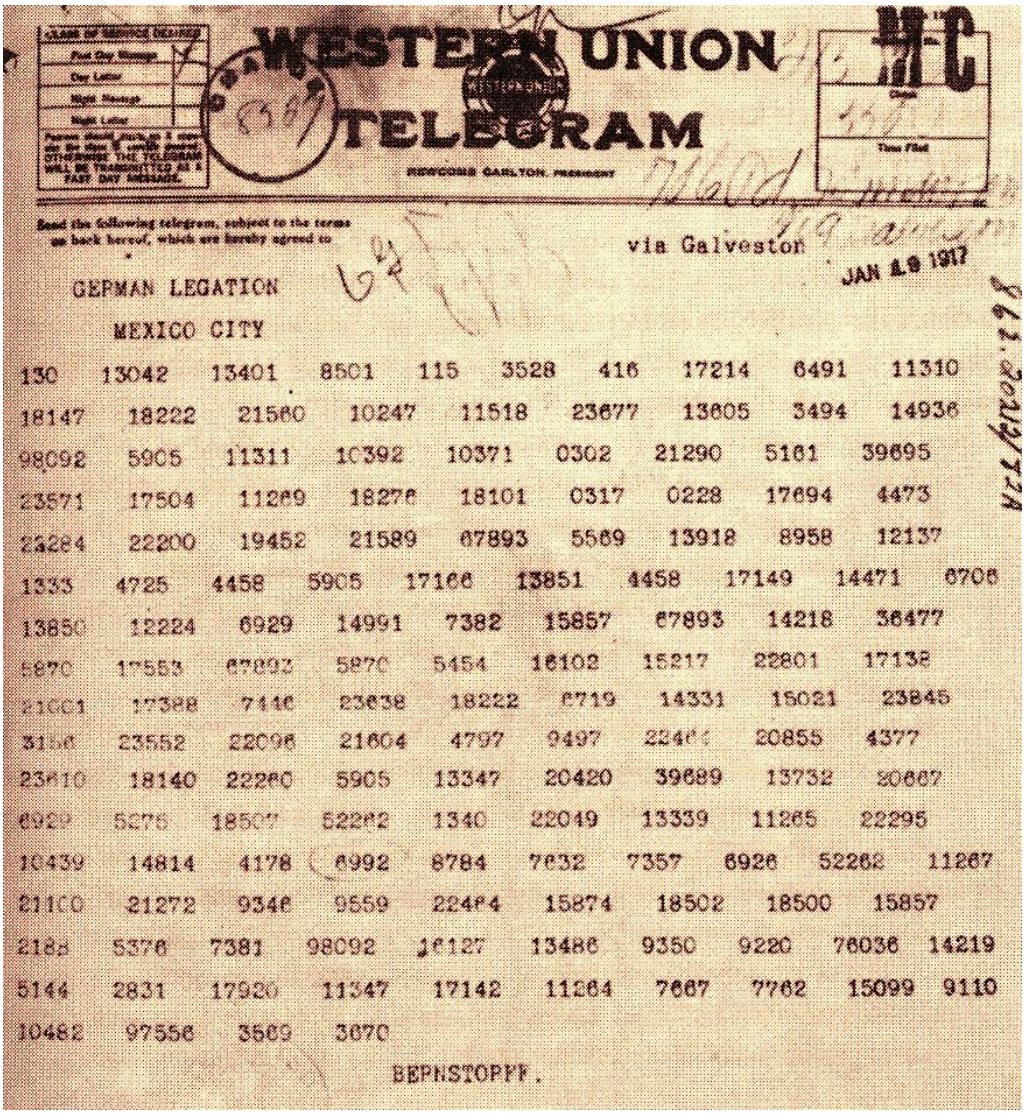
Fonte: Elaborado pelo autor.

1.3 O TELEGRAMA ZIMMERMANN E A GUERRA

O telegrama de Zimmermann continha uma mensagem do então Ministro do Exterior Alemão Arthur Zimmermann para o seu embaixador no México, só que o telegrama foi interceptado e decifrado em janeiro de 1917 (período em que ocorria a 1º Guerra Mundial) pelos criptógrafos britânicos Nigel de Grey e William Montgomery.

Zimmermann instruiu seu embaixador a oferecer significativa ajuda financeira ao México para que o país entrasse como aliado da Alemanha na hipótese de um conflito contra os EUA, fato esse que fez os EUA entrarem na Guerra após três anos de seu início.

Figura 3 – Telegrama de Zimmermann



WESTERN UNION TELEGRAM

via Galveston JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
24284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7110 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5870 18500 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

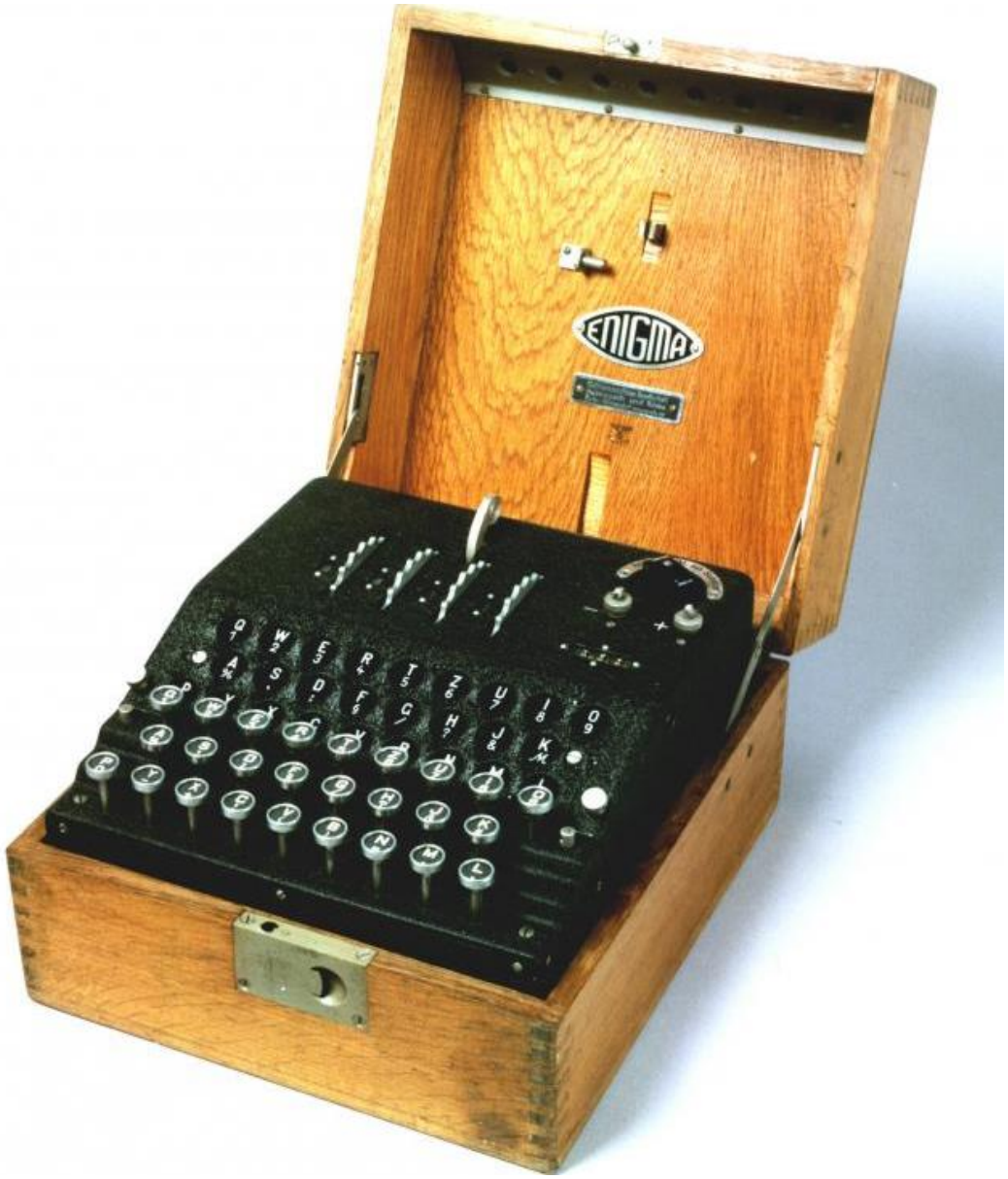
Disponível em: https://br.pinterest.com/robran2012/wwi/. Acesso em: 13 out 2016.

1.4 O PASSADO RECENTE

A primeira guerra mundial mostrou a importância da criptografia no campo de batalha, e o perigo da criptografia decifrada facilmente, sendo desenvolvidos a partir de então códigos 'inquebráveis'. A Segunda Guerra Mundial se tornou um momento decisivo na história da criptografia e colocou-a diretamente no centro da estratégia militar e política desde aquela época até os dias atuais.

Nesse período foi criada a máquina ENIGMA, que foi desenvolvida pelo alemão Arthur Sherbius utilizada tanto para criptografar como para descriptografar códigos de guerra, foi bastante utilizada pelo exército alemão durante a 2º Guerra Mundial, porém seu código foi decifrado, pelo britânico Alan Mathison Turing, grande matemático e considerado o pai da computação moderna, e as informações contida nas mensagens descriptografadas são tidas como responsáveis pelo fim da Segunda Guerra Mundial pelo menos um ano antes do previsto, fato relatado no filme ‘O Jogo da Imitação’.

Figura 4 – Máquina Enigma usada na 2º Guerra Mundial



Disponível em: https://www.bletchleypark.org.uk/calendar/event_detail.rhtm?recID=56786. Acesso em: 13 out 2016.

1.5 O COMEÇO DA EVOLUÇÃO

A década de 1980 e anos 90 evoluíram em um mundo digital. O advento do microprocessador e do computador pessoal e sua aceitação em todos os dias de vida significa que cada vez mais nossas vidas privadas, é digital. Esse dialeto digital gerou uma vasta rede de comunicações tais como: a internet, telefones celulares, terminais de autoatendimento, e vários aplicativos de mensagens instantânea, oferecendo uma comunicação segura, como é o caso do *Whatsapp*, um aplicativo usado hoje por aproximadamente um bilhão de usuários e que usa como segurança de suas mensagens a criptografia.

1.6 CIFRA DE SUBSTITUIÇÃO E A CIFRA DE CÉSAR

Umas das cifras mais conhecidas é a Cifra de César, também conhecida como cifra de troca, código de César ou troca de César, é uma das mais simples técnicas de substituição criptográficas, foi usada por Júlio César para se comunicar com seus generais em períodos de guerra.

Essa técnica consiste em uma simples substituição da letra de um texto por outra do alfabeto de acordo com a tabela abaixo:

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M
Cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P

Normal	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Uma mensagem como: MATEMÁTICA E A CRIPTOGRAFIA seria cifrada como PDWHPDWLFD H D FULSWRJUDILD.

No caso da cifra de substituição em si, temos uma chave criada aleatoriamente, ou seja, podemos substituir cada letra de um texto por uma letra qualquer, fazendo agora uma análise de quantas chaves podemos ter nessa cifra vemos que temos 26! possibilidades de chaves.

Agora com a seguinte tabela vamos criar o texto anterior cifrado:

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

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

Texto Cifrado: PUHAPUHEYU A U YKEMHIVKEU

Texto Original: MATEMATICA E A CRIPTOGRAFIA

Podemos também usar esse tipo de cifras através da substituição das letras do alfabeto por números, mais para se tornar algo mais simples de se entender, no caso a seguir fizemos substituição trocando cada letra na sequência numérica de 1 a 26, da seguinte forma:

Normal	A	B	C	D	E	F	G	H	I	J	K	L	M
Cifrado	1	2	3	4	5	6	7	8	9	10	11	12	13

Normal	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifrado	14	15	16	17	18	19	20	21	22	23	24	25	26

Ou seja, a palavra PROFMAT, pode ser cifrada usando a tabela anterior:

P	R	O	F	M	A	T
16	18	15	6	13	1	20

É claro que podemos incrementar um pouco mais a chave usada para cifrar um texto, sendo assim usaremos agora a tabela a seguir para cifrarmos outras palavras:

Tabela 1: Base para criptografia de substituição

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
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
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	2
4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3
5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5
7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6
8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7
9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11
13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12
14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13
15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
26	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

Fonte: Elaborada pelo autor.

Veja que na tabela cada letra do alfabeto será trocada por um número de 1 a 26, só que em todas as linhas isso é feito de forma sequencial e não aleatória, o que significa que se você escolhe por exemplo a letra “O” como o número 1, a “P” automaticamente será substituída pelo 2, e assim por diante.

Vejamos um exemplo, para descriptografar a palavra cifrada:

4	17	2	20	5

Veja que mesmo sabendo que as linhas seguem uma sequência numérica, não temos tanta facilidade em descobrir a palavra acima, mas note que para que isso se torne algo mais simples devemos ter a informação de qual linha da tabela 1 foi utilizada

para criptografar a palavra, ou seja, nossa chave já não é tão simples de ser desvendada.

Só que nesse caso específico a linha usada para criptografar a palavra foi a 16, significando que a letra “A” é representada pelo número 16:

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
16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Sendo assim, podemos agora facilmente substituir os números pelas suas respectivas letras:

4	17	2	20	5
O	**B**	**M**	**E**	**P**

1.7 CIFRA DE HILL

Foi inventada pelo matemático norte americano Lester S. Hill em 1929, ela é baseada na troca de letras do alfabeto por números e usa como chave matrizes quadradas invertíveis.

Algo muito similar será mostrado no item aplicação de matrizes a criptografia.

2 FUNÇÕES E A CRIPTOGRAFIA

Nesta seção abordaremos o conceito de função, mostrando onde são aplicadas, além de conceitos de função composta e função inversa, os quais serão mais adiante utilizados para relacionar a criptografia e a função.

2.1 CONCEITO DE FUNÇÃO

A função é um dos tópicos mais importantes na matemática, seu conceito está relacionado com a associação de conjuntos, através da ligação entre grandezas, o professor Elon Lages Lima no livro “A Matemática do Ensino Médio – Vol. 1”- apresenta a seguinte definição:

> *[1] Dados os conjuntos X, Y, uma função f: X →Y (lê-se “uma função de X em Y”) é uma regra (ou conjunto de instruções) que diz como associar a cada elemento x ∈ X um elemento y = f(x) ∈ Y. O conjunto X chama-se domínio e Y é o contradomínio da função f. Para cada x ∈ X, o elemento f(x) ∈ Y chama-se a imagem de x pela função f, ou o valor assumido pela função f no ponto x ∈ X. Escreve-se x ↦ f(x) para indicar que f transforma (ou leva) x em f(x).*

Após conversa com professores tanto de escola pública quanto privada, tentamos absorver como esse conceito era trabalhado em sala de aula. Adotamos aqui a forma que acreditamos ser mais proveitosa, na qual a função é introduzida através de situações problemas simples, uma maneira de estimular o aluno raciocinar. Exemplo:

Imagine que ao você entrar em um táxi, o taxímetro já registre como taxa fixa R$ 6,00, e que seja acrescentado por km mais R$ 1,50 de segunda a sexta feira durante o dia e R$ 2,25 durante a noite, finais de semana e feriados, sendo assim, responda:

a) Em uma corrida de 12 km e 18 Km em uma manhã de segunda feira, quais os valores a serem pagos?
b) Em uma corrida de 20 km e 16 km de um fim de semana, quais os valores a serem pagos?

c) O valor de uma corrida no domingo foi R$ 35,25, qual a distância percorrida pelo táxi?

d) O valor de uma corrida na quarta-feira pela manhã foi de R$ 21,00, quanto o táxi percorreu?

e) Quais as fórmulas matemáticas servem para relacionar o valor a ser pago y com a distância x percorrida pelo táxi?

Solução:

Corrida de segunda a sexta de dia		
Distância percorrida (x em KM)	Cálculo do Valor a ser pago (y em Reais)	Valor pago
0	$6 + 1{,}50.0$	R$ 6,00
1	$6 + 1{,}50.1$	R$ 7,50
2	$6 + 1{,}50.2$	R$ 9,00
3	$6 + 1{,}50.3$	R$ 10,50
12	$6 + 1{,}50.12$	R$ 24,00
18	$6 + 1{,}50.18$	R$ 33,00
x	$6 + 1{,}50.x$	y

Corridas a noite, fins de semana e feriado		
Distância percorrida (x em KM)	Cálculo do Valor a ser pago (y em Reais)	Valor pago
0	$6 + 2{,}25.0$	R$ 6,00
1	$6 + 2{,}25.1$	R$ 8,25
2	$6 + 2{,}25.2$	R$ 10,50
3	$6 + 2{,}25.3$	R$ 12,75
16	$6 + 2{,}25.16$	R$ 42,00
20	$6 + 2{,}25.20$	R$ 51,00
x	$6 + 2{,}25.x$	y

a) Na corrida de 12 km deve ser pago R$ 24,00 e na de 18 km R$ 33,00.

b) Na corrida de 16 km deve ser pago R$ 42,00 e na de 20 km R$ 51,00.

c) Para encontrarmos a distância percorrida temos que encontrar o valor de x quando $6 + 2{,}25.x$ for igual a R$ 35,25, ou seja,

$$6 + 2{,}25.x = 35{,}25$$
$$2{,}25.x = 35{,}25 - 6$$
$$x = 29{,}25/2{,}25$$
$$x = 13 \text{ km}$$

d) Para encontrarmos a distância percorrida temos que encontrar o valor de x quando $6 + 1{,}50.x$ for igual a R$ 21,00, ou seja,

$$6 + 1{,}50.x = 21{,}00$$
$$1{,}50.x = 21{,}00 - 6$$
$$x = 15{,}00/1{,}50$$
$$x = 10 \text{ km}$$

e) Nas tabelas encontramos as duas funções procuradas:

$y = 6 + 1{,}50.\, x$
$y = 6 + 2{,}25.\, x$

A função representa então a variação que uma determinada grandeza tem em função da outra, podemos ver isso diariamente em nosso cotidiano, ao pagar o táxi, o valor pago depende da distância percorrida, ao pagar uma conta de energia, pagamos de acordo com kwh consumido durante o mês, o preço pago por uma quantidade de carne depende do valor do quilo na compra, a quantidade de cerâmica consumida para colocar em um cômodo da sua casa está em função das dimensões deste cômodo, o lucro de uma empresa que trabalha com vendas, depende de algumas variáveis como o valor gasto na aquisição do seu produto, além do valor investido com colaboradores, ou seja, a função é algo que usamos no nosso cotidiano, por isso a importância no seu estudo.

O conteúdo de função é muito amplo, temos neles o conceito, definições de domínio, imagem e contradomínio, construção e leituras de gráficos, funções injetoras, sobrejetora e bijetoras, suas propriedades, funções compostas e inversas, além de aprendermos sobre os vários tipos de funções (afim, quadrática, exponencial, logarítmica, trigonométrica e outras mais), porém aqui vamos nos limitar a partir de agora, fazer a análise das propriedades da função composta e função inversa.

2.2 FUNÇÕES COMPOSTAS E FUNÇÕES INVERSAS

2.2.1 Função composta

Sejam duas funções g e f, definimos as funções composta de g com f, gof e de f com g, fog, como sendo:

$(gof)(x) = g\big(f(x)\big)$

$(fog)(x) = f\big(g(x)\big)$

Podemos verificar que a operação de função composta não é comumativa, ou seja,

$(gof)(x) \neq (fog)(x)$

Exemplo:

Dada as funções definidas por $f(x) = 2x - 1$ *e* $g(x) = x^2$

Determine:

a) $(fog)(x)$
b) $(gof)(x)$

Solução:

a) Consideremos que $(fog)(x) = f\big(g(x)\big)$, temos então:

$$f\big(g(x)\big) = f(x^2) = 2(x^2) - 1 = 2x^2 - 1$$

b) Consideremos que $(gof)(x) = g\big(f(x)\big)$, temos então:

$$g\big(f(x)\big) = g(2x - 1) = (2x - 1)^2 = 4x^2 - 4x + 1$$

As soluções servem para mostrar que de fato que a operação de função composta não é comumativa.

2.2.2 Função Inversa

Considerando que f seja uma função inversível, definimos a função inversa de f, a função f^{-1}, de tal forma que:

$$(fof^{-1})(x) = (f^{-1}of)(x) = x,$$

Ou seja, quando a função f composta com f^{-1} e vice e versa, leva-nos à função identidade.

Exemplo:

Dada a função definida por $f(x) = 2x - 1$, determine f^{-1}.

Solução:

Substituindo $f(x)$ por y e posteriormente isolamos x na equação temos:

$y = 2x - 1$

$$x = \frac{y+1}{2}$$

Agora trocamos x por y e y por x:

$$y = \frac{x+1}{2}$$

Assim:

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

Fazendo agora

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

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

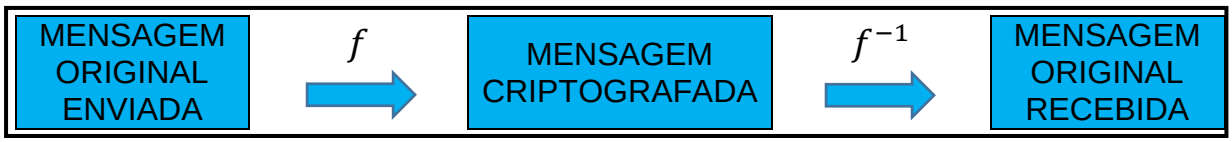
Verificamos assim que:

$$(fof^{-1})(x) = (f^{-1}of)(x) = x$$

2.3 APLICAÇÃO DE FUNÇÃO EM CRIPTOGRAFIA

De um modo geral podemos perceber que o objetivo do processo criptográfico é ‘esconder’ as chaves que transformam uma mensagem normal em uma codificada, relacionando essa chave com uma função, podemos escrever esse processo da seguinte forma:

Figura 5 – Processo de Criptografia usando funções



Fonte: Elaborada pelo autor

Ou seja, o nosso processo terá uma função para criptografar a mensagem e sua inversa para retornar a original.

Nesse caso, trabalharemos com funções afins e com a tabela 1, usada na seção anterior, assim sendo teremos algo mais ‘escondido’ por que além de uma pessoa que procure interceptar a mensagem ter que saber a função utilizada, terá que ter conhecimento da linha que foi usada no processo.

Vejamos o seguinte exemplo:

João e Maria decidiram trocar mensagens criptografadas utilizando o processo descrito anteriormente, sendo que usaram a primeira linha da tabela 1, e a função $f(x) = 3x - 1$ como chave, assim sendo João decide enviar para Maria a seguinte mensagem:

MATEMÁTICA É A RAINHA DAS CIÊNCIAS

Que está relacionada com a seguinte sequência numérica (usaremos sempre o número zero como espaço):

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

13 1 20 5 13 1 20 9 3 1 0 5 0 1 0 18 1 9 14 8 1 0 4 1 19 0 3 9 5 14 3 9 1 19

João então começa a criptografar a mensagem:

$f(13) = 3.13 - 1 = 38$, $f(1) = 3.1 - 1 = 2$, $f(20) = 3.20 - 1 = 59$, $f(5) = 3.5 - 1 = 14$ e assim por diante, até que envia para Maria a seguinte mensagem:

38 2 59 14 38 2 59 26 8 2 -1 14 -1 2 -1 53 2 26 41 23 2 -1 11 2 56 -1 8 26 14 41 8 26 2 56

Após receber a mensagem Maria começa a fazer o processo inverso, utilizando a função inversa:

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

E assim por diante, após fazer todo o processo Maria conseguiu ler a mensagem enviada por João. Fazendo a substituição da mensagem em f^{-1} temos:

$$f^{-1}(38) = \frac{38+1}{3} = 13 = \boldsymbol{M}$$

$$f^{-1}(2) = \frac{2+1}{3} = 1 = \boldsymbol{A}$$

$$f^{-1}(59) = \frac{59+1}{3} = 20 = \boldsymbol{T}$$

$$f^{-1}(14) = \frac{14+1}{3} = 5 = \boldsymbol{E}$$

3 MATRIZES E A CRIPTOGRAFIA

Nesta seção abordaremos o conceito de matrizes, os nome especiais que cada uma recebe, operações com matrizes, além da definição de determinantes de matrizes e matriz inversa, conceitos esses que foram utilizados para relacionar a criptografia e matrizes.

3.1 CONCEITO E REPRESENTAÇÃO

Vejamos a seguinte tabela:

Tabela 2: Tabela de cotação do produto X, de janeiro de 2011 a dezembro de 2016.

Mês/ano	2011	2012	2013	2014	2015	2016
Janeiro	R$ 126,32	R$ 137,69	R$ 152,83	R$ 162,00	R$ 158,76	R$ 168,29
Fevereiro	R$ 142,00	R$ 154,78	R$ 171,81	R$ 182,11	R$ 178,47	R$ 189,18
Março	R$ 156,20	R$ 170,26	R$ 188,99	R$ 200,33	R$ 196,32	R$ 208,10
Abril	R$ 141,20	R$ 153,91	R$ 170,84	R$ 181,09	R$ 177,47	R$ 188,11
Maio	R$ 139,50	R$ 152,06	R$ 168,78	R$ 178,91	R$ 175,33	R$ 185,85
Junho	R$ 136,00	R$ 148,24	R$ 164,55	R$ 174,42	R$ 170,93	R$ 181,19
Julho	R$ 133,25	R$ 145,24	R$ 161,22	R$ 170,89	R$ 167,47	R$ 177,52
Agosto	R$ 130,75	R$ 142,52	R$ 158,19	R$ 167,69	R$ 164,33	R$ 174,19
Setembro	R$ 129,36	R$ 141,00	R$ 156,51	R$ 165,90	R$ 162,59	R$ 172,34
Outubro	R$ 129,00	R$ 140,61	R$ 156,08	R$ 165,44	R$ 162,13	R$ 171,86
Novembro	R$ 128,44	R$ 140,00	R$ 155,40	R$ 164,72	R$ 161,43	R$ 171,11
Dezembro	R$ 128,00	R$ 139,52	R$ 154,87	R$ 164,16	R$ 160,88	R$ 170,53

Fonte: Elaborada pelo autor.

Matriz mxn é uma tabela formada por m linhas e n colunas, no caso da tabela anterior, m representa os meses do ano, e n os anos, podendo ser representada por uma matriz A do tipo 12x6 (com doze linhas e seis colunas) como a seguir:

$$A = \begin{bmatrix} 126{,}32 & 137{,}69 & 152{,}83 & 162{,}00 & 158{,}76 & 168{,}29 \\ 142{,}00 & 154{,}78 & 171{,}81 & 182{,}11 & 178{,}47 & 189{,}18 \\ 156{,}20 & 170{,}26 & 188{,}99 & 200{,}33 & 196{,}32 & 208{,}10 \\ 141{,}20 & 153{,}91 & 170{,}84 & 181{,}09 & 177{,}47 & 188{,}11 \\ 139{,}50 & 152{,}06 & 168{,}78 & 178{,}91 & 175{,}33 & 185{,}85 \\ 136{,}00 & 148{,}24 & 164{,}55 & 174{,}42 & 170{,}93 & 181{,}19 \\ 133{,}25 & 145{,}24 & 161{,}22 & 170{,}89 & 167{,}47 & 177{,}52 \\ 130{,}75 & 142{,}52 & 158{,}19 & 167{,}69 & 164{,}33 & 174{,}19 \\ 129{,}36 & 141{,}00 & 156{,}51 & 165{,}90 & 162{,}59 & 172{,}34 \\ 129{,}00 & 140{,}61 & 156{,}08 & 165{,}44 & 162{,}13 & 171{,}86 \\ 128{,}44 & 140{,}00 & 155{,}40 & 164{,}72 & 161{,}43 & 171{,}11 \\ 128{,}00 & 139{,}52 & 154{,}87 & 164{,}16 & 160{,}88 & 170{,}53 \end{bmatrix}$$

De forma a generalizar uma matriz mxn, podemos escrever da seguinte forma:

$$B = \begin{bmatrix} b_{11} & b_{12} & b_{13} & \cdots & b_{1j} \\ b_{21} & a_{22} & b_{23} & \cdots & b_{2j} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ b_{i1} & b_{i2} & b_{i3} & \cdots & b_{ij} \end{bmatrix}$$

De forma que as matrizes são representadas por letras maiúsculas, seus elementos acompanhados dos índices que representam a linha e a coluna, por exemplo o elemento a_{53} da matriz A, está posicionado na quinta linha e terceira coluna, que no caso da Matriz A é o elemento 168,78.

3.2 TIPOS DE MATRIZES

Temos algumas matrizes que recebem nomes especiais:

a) Matriz linha: é toda matriz do tipo 1xn, ou seja, com uma linha e n colunas.
   Exemplo:
   $L = [12 \quad 5 \quad 1]$, matriz (1x3)

b) Matriz coluna: é toda matriz do tipo mx1, ou seja, com m linhas e 1 coluna.
   Exemplo:
   $C = \begin{bmatrix} 7 \\ 11 \\ 16 \end{bmatrix}$, matriz C (3x1)

c) Matriz nula: é a matriz em que todos os seus elementos são nulos.
   Exemplo:
   $N = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, matriz nula N (2x3)

d) Matriz transposta: representamos como a matriz transposta de A, a matriz A^t de tal forma que os elementos da matriz A que estavam na linha passam a estar na coluna da matriz A^t, ou seja, uma matriz mxn tem uma transposta nxm.
   Exemplo:
   $A = \begin{bmatrix} 7 & 5 & 12 \\ 6 & 3 & 9 \end{bmatrix}$, matriz A (2x3)
   $A^t = \begin{bmatrix} 7 & 6 \\ 5 & 3 \\ 12 & 9 \end{bmatrix}$, matriz A^t (3x2)

e) Matriz quadrada: é toda matriz em que seu número de linhas é igual ao número de colunas, ou seja, uma matriz do tipo nxn, falamos que essa matriz é da ordem n.

Exemplo:

$$C = \begin{bmatrix} 6 & 2 & 12 \\ 4 & 0 & 3 \\ 9 & 8 & 7 \end{bmatrix}$$ matriz C do tipo (3x3), ou ordem 3

Nas matrizes quadradas aparecem também os conceitos de diagonal principal e diagonal secundaria.

A diagonal principal é a diagonal que contém os elementos c_{ii}, ou seja, na matriz C anterior, a diagonal principal é formada pelos elementos $c_{11} = 6, c_{22} = 0$ *e* $c_{33} = 7$.

Já a diagonal secundária é representada pelos elementos c_{ij}, de tal forma que, $i + j = n + 1$, na matriz C a diagonal secundária é representada pelos elementos $c_{13} = 12, c_{22} = 0$ *e* $c_{31} = 9$.

f) Matriz identidade: é uma matriz quadrada em que todos os elementos da diagonal principal é um (1) e os elementos que não pertencem a diagonal principal são nulos.

Exemplo:

$C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, matriz identidade de ordem 3.

3.3 OPERAÇÃO COM MATRIZES

3.3.1 Adição e subtração de matrizes

Duas matrizes A e B só podem ser somadas ou subtraídas, se e somente se, ambas tiverem o mesmo número de linhas e colunas.

Dada duas matrizes A e B, adição de matrizes é feita através da soma dos elementos correspondentes, ou seja, $a_{ij} + b_{ij}$.

A adição e subtração de matrizes são: associativas, comutativa, tem um elemento neutro e um oposto.

Exemplo:

$$\begin{bmatrix}7 & 5 & 12\\ 6 & 3 & 9\end{bmatrix}+\begin{bmatrix}1 & -3 & 1\\ 4 & -5 & 2\end{bmatrix}=\begin{bmatrix}7+1 & 5+(-3) & 12+1\\ 6+4 & 3+(-5) & 9+2\end{bmatrix}=\begin{bmatrix}8 & 2 & 13\\ 10 & -2 & 11\end{bmatrix}$$

A subtração é análoga a adição, feita com seus elementos correspondentes.

Exemplo:

$$\begin{bmatrix}7 & 5 & 12\\ 6 & 3 & 9\end{bmatrix}-\begin{bmatrix}1 & -3 & 1\\ 4 & -5 & 2\end{bmatrix}=\begin{bmatrix}7-1 & 5-(-3) & 12-1\\ 6-4 & 3-(-5) & 9-2\end{bmatrix}=\begin{bmatrix}6 & 8 & 11\\ 2 & 8 & 7\end{bmatrix}$$

3.3.2 Multiplicação de um número real por matriz

Dado um número real qualquer $\propto$ e uma matriz A_{mxn}, o produto $\propto . A$ é obtida pela multiplicação de cada elemento de A por $\propto$.

A multiplicação de um número real por uma matriz, tem as seguintes propriedades: associativa, distributiva e tem um elemento neutro.

Exemplo:

$$2.\begin{bmatrix}7 & 5 & 12\\ 6 & 3 & 9\end{bmatrix}=\begin{bmatrix}14 & 10 & 24\\ 12 & 6 & 18\end{bmatrix}$$

3.3.3 Multiplicação de matrizes

O produto entre matrizes só é possível se o número de colunas da primeira for igual ao número de linhas da segunda matriz, ou seja, podemos ter duas matrizes com mesmas dimensões que nem sempre será possível realizar o produto entre ambas.

O produto é feito da seguinte forma, dada duas matrizes A_{mxn} e B_{nxp}, teremos como resultado a matriz C_{mxp}, onde cada elemento da matriz C_{mxp} tem a seguinte lei de formação:

$c_{11} = a_{11}.b_{11} + a_{12}.b_{21} + a_{13}.b_{31} + \cdots + a_{1n}.b_{n1}$

$$c_{12} = a_{11}.b_{12} + a_{12}.b_{22} + a_{13}.b_{32} + \cdots + a_{1n}.b_{n2}$$
$$c_{13} = a_{11}.b_{13} + a_{12}.b_{23} + a_{13}.b_{33} + \cdots + a_{1n}.b_{n3}$$
$$c_{1p} = a_{11}.b_{1p} + a_{12}.b_{2p} + a_{13}.b_{3p} + \cdots + a_{1n}.b_{np}$$
$$\vdots$$
$$c_{mp} = a_{m1}.b_{1p} + a_{m2}.b_{2p} + a_{m3}.b_{3p} + \cdots + a_{mn}.b_{np}$$

O produto de matrizes tem as seguintes propriedades: associativa, distributiva em relação a adição e tem um elemento neutro.

Exemplos:

Dadas as matrizes $A = \begin{bmatrix} 1 & 4 & 3 \\ 0 & -2 & 9 \end{bmatrix}$ e $B = \begin{bmatrix} 7 & 2 \\ 5 & -3 \\ 1 & 1 \end{bmatrix}$, vejamos como serão feitos os produtos $AxB\ e\ BxA$:

$$AxB = \begin{bmatrix} 1.7 + 4.5 + 3.1 & 1.2 + 4.-3 + 3.1 \\ 0.7 + (-2).5 + 9.1 & 0.2 + (-2).(-3) + 9.1 \end{bmatrix} = \begin{bmatrix} 30 & -7 \\ -1 & 15 \end{bmatrix}$$

$$BxA = \begin{bmatrix} 7.1 + 2.0 & 7.4 + 2.(-2) & 7.3 + 2.9 \\ 5.1 + (-3).0 & 5.4 + (-3).(-2) & 5.3 + (-3).9 \\ 1.1 + 1.0 & 1.4 + 1.(-2) & 1.3 + 1.9 \end{bmatrix} = \begin{bmatrix} 7 & 24 & 39 \\ 5 & 26 & -12 \\ 1 & 2 & 12 \end{bmatrix}$$

Podemos verificar que a multiplicação de matrizes não é comutativa, ou seja, $AXB \neq BXA$

3.4 DETERMINANTES DE MATRIZES

O determinante está relacionado com uma matriz quadrada, desempenhando importante papel para cálculo de matriz inversa, resolução de sistemas lineares e cálculo de áreas de triângulos quando se conhece seus pontos. O determinante de uma matriz A será denotado det (A) ou |A|.

O determinante de uma matriz de primeira ordem é o próprio elemento da matriz.

Exemplo: Dada a matriz $A = [5]$, temos que $\det(A) = 5$.

3.4.1 Determinante de uma matriz 2x2

Dada a matriz uma matriz $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, o determinante dessa matriz é definido como:

$det(A) = a_{11}.a_{22} - a_{12}.a_{21}$

Exemplo: Sendo $A = \begin{bmatrix} 5 & 2 \\ 3 & 2 \end{bmatrix}$, $det(A) = 5.2 - 2.3 = 4$

$det(A) = 4$

3.4.2 Determinante de uma matriz 3x3

Dada a matriz uma matriz $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$, o determinante dessa matriz é definido como:

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

Exemplo: Sendo $A = \begin{bmatrix} -3 & 2 & 5 \\ 0 & 1 & 2 \\ 3 & 2 & 1 \end{bmatrix}$,

$det(A) = -3.\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} - 2.\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} + 5.\begin{bmatrix} 0 & 1 \\ 3 & 2 \end{bmatrix}$

$det(A) = -3.(-3) - 2.(-6) + 5.(-3)$

$det(A) = 6$

3.4.3 Determinante de uma matriz nxn

Para o caso geral, onde A é uma matriz n × n, o determinante é dado por:

$det(A) = a_{11}.\alpha_{11} + a_{12}.\alpha_{12} + a_{13}.\alpha_{13} + \cdots + a_{1n}.\alpha_{1n}$

Onde:

$\alpha_{1n} = (-1)^{i+j}\beta_{ij}$ (é o que chamamos de cofator)

E β_{ij} é o menor complementar referente a a_{ij}, é representado pelo determinante da matriz suprimida de A, retirando-se o elementos da linha e da coluna que está o elemento a_{ij}.

Exemplo: Sendo a matriz $C = \begin{bmatrix} -3 & 2 & 5 \\ 0 & 1 & 2 \\ 3 & 2 & 1 \end{bmatrix}$, o menor complementar do elemento $a_{12} = 2$ é o determinante da matriz C sem os elementos em destaque $\begin{bmatrix} -3 & 2 & 5 \\ 0 & 1 & 2 \\ 3 & 2 & 1 \end{bmatrix}$, ou seja, o determinante da matriz $\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} = -6$.

Assim podemos determinar a matriz dos cofatores representada por $\bar{A}$, que é uma matriz formada pelo cofator de cada elemento da matriz.

E a transposta da matriz dos cofatores de uma matriz A é o que chamamos de matriz adjunta representada por $(\bar{A})^t$ ou $Adj\ (A)$.

O nome do método inserido para o cálculo do determinante de uma matriz de ordem n, é o que chamamos de Teorema de Laplace, temos ainda muitos outros métodos para o cálculo do determinante como: Regra de Sarrus, regra de Chió, Determinante da Matriz de Vandermonde, propriedades e teoremas que não serão inseridos aqui.

3.5 DETERMINANTES IGUAIS A ZERO

O determinante de uma matriz será zero se:

a) Todos os elementos de uma fila (linha ou coluna) forem nulos.
b) Duas filas forem iguais.
c) Uma linha for proporcional a outra fila.
d) Os elementos de uma fila forem combinação linear de outras filas

3.6 MATRIZ INVERSA

Supondo uma matriz A de ordem n, define-se como a inversa de A, a matriz A^{-1}, de tal forma que:

$$A.A^{-1} = A^{-1}.A = I$$

onde I é a matriz identidade de ordem n.

Para o cálculo da matriz inversa A^{-1} de A usamos a seguinte equação:

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

Daí concluímos que não existe matriz inversa de uma matriz em que seu determinante é zero, quando isso ocorre a matriz recebe o nome de matriz singular.

Exemplo: Sendo a matriz $A = \begin{bmatrix} 1 & 2 \\ 5 & 9 \end{bmatrix}$, mostraremos passo a passo o cálculo da matriz A^{-1}:

a) Primeiro encontrar o $det(A)$:

$det(A) = 1.9 - 5.2 = 9 - 10 = -1$

Dessa forma verificamos que a matriz tem uma inversa.

b) Agora encontraremos o cofator de cada elemento:

$\alpha_{11} = (-1)^{1+1}\beta_{11} = 9$

$\alpha_{12} = (-1)^{1+2}\beta_{12} = -5$

$\alpha_{21} = (-1)^{2+1}\beta_{21} = -2$

$\alpha_{22} = (-1)^{2+2}\beta_{22} = 1$

c) Busca pela matriz adjunta

Lembrando que a matriz adjunta é a transposta da matriz dos cofatores, ou seja, a transposta da matriz $\bar{A} = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} = \begin{bmatrix} 9 & -5 \\ -2 & 1 \end{bmatrix}$, que no caso é a matriz $adj(A) = \begin{bmatrix} 9 & -2 \\ -5 & 1 \end{bmatrix}$

Agora basta substituir na equação

$A^{-1} = \frac{1}{det(A)}.adj(A) = \frac{1}{-1}.\begin{bmatrix} 9 & -2 \\ -5 & 1 \end{bmatrix} = \begin{bmatrix} -9 & 2 \\ 5 & -1 \end{bmatrix}$

De fato, fazendo o produto $A.A^{-1} = I$

$A.A^{-1} = \begin{bmatrix} 1 & 2 \\ 5 & 9 \end{bmatrix}.\begin{bmatrix} -9 & 2 \\ 5 & -1 \end{bmatrix} = \begin{bmatrix} -9+10 & 2-2 \\ -45+45 & 10-9 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

3.7 APLICAÇÃO DE MATRIZES E CRIPTOGRAFIA

Como já mencionamos anteriormente a criptografia tem o objetivo de ‘esconder’ as chaves que codificam uma mensagem. E nesse caso específico, relacionando a nossa chave com uma matriz, escrevemos o processo da seguinte forma:

Figura 6 – Processo de criptografia usando matrizes.

Fonte: Elaborada pelo autor

Ou seja, neste processo transformaremos uma mensagem original em uma matriz M, usaremos uma matriz A qualquer para codificar a mensagem e posteriormente a inversa de A para retornarmos a mensagem original.

Usaremos esse método baseado nas seguintes propriedades de Matrizes:

$M.I = M$ (elemento neutro da multiplicação, matriz identidade)

$(M.A).A^{-1} = M$ (propriedade associativa da multiplicação).

Vejamos um exemplo:

Seja $M = \begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix}$ e $A = \begin{bmatrix} 5 & 3 \\ 2 & 1 \end{bmatrix}$ então o produto $A.B$ será:

$M.A = \begin{bmatrix} 1.5+2.2 & 1.3+2.1 \\ 3.5+8.2 & 3.3+8.1 \end{bmatrix} = \begin{bmatrix} 9 & 5 \\ 31 & 17 \end{bmatrix}$ agora fazendo $(M.A).A^{-1}$ e sabendo que $A^{-1} = \begin{bmatrix} -1 & 3 \\ 2 & -5 \end{bmatrix}$temos:

$$\begin{bmatrix} 9 & 5 \\ 31 & 17 \end{bmatrix}.\begin{bmatrix} -1 & 3 \\ 2 & -5 \end{bmatrix} = \begin{bmatrix} 9.(-1)+5.2 & 9.3+5.(-5) \\ 31.(-1)+17.2 & 31.3+17.(-5) \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix} = M$$

Ou seja, o produto $(M.A).A^{-1} = M$

Como exemplo de aplicação usaremos a mesma frase usada no capítulo 3.

MATEMÁTICA É A RAINHA DAS CIÊNCIAS

Usaremos a primeira linha da tabela 1, que está relacionada com a seguinte sequência numérica (usaremos sempre o número zero como espaço):

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

13 1 20 5 13 1 20 9 3 1 0 5 0 1 0 18 1 9 14 8 1 0 4 1 19 0 3 9 5 14 3 9 1 19

Transformando essa matriz em uma matriz M com três colunas temos:

$$M = \begin{bmatrix} 13 & 1 & 20 \\ 5 & 13 & 1 \\ 20 & 9 & 3 \\ 1 & 0 & 5 \\ 0 & 1 & 0 \\ 18 & 1 & 9 \\ 14 & 8 & 1 \\ 0 & 4 & 1 \\ 19 & 0 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \\ 19 & 0 & 0 \end{bmatrix}$$

Como chave usaremos a matriz $A = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix}$ (ao escolhermos a matriz chave tomamos o cuidado de não escolher uma matriz singular) fazendo então $M.A$ teríamos:

$$\begin{bmatrix} 13 & 1 & 20 \\ 5 & 13 & 1 \\ 20 & 9 & 3 \\ 1 & 0 & 5 \\ 0 & 1 & 0 \\ 18 & 1 & 9 \\ 14 & 8 & 1 \\ 0 & 4 & 1 \\ 19 & 0 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \\ 19 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 \\ 2 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 15 & 2 & 35 \\ 31 & 26 & 32 \\ 38 & 18 & 41 \\ 1 & 0 & 6 \\ 2 & 2 & 2 \\ 20 & 2 & 29 \\ 30 & 16 & 31 \\ 8 & 8 & 9 \\ 19 & 0 & 22 \\ 19 & 10 & 33 \\ 21 & 18 & 22 \\ 19 & 0 & 19 \end{bmatrix}$$

A mensagem criptografada ficaria:

15 2 35 31 26 32 38 18 41 1 0 6 2 2 2 20 2 29 30 16 31 8 8 9 19 0 22 19 10 33 21 18 22 19 0 19

Imaginemos agora o inverso, recebemos a mensagem criptografada a cima, como fazer para encontrar a mensagem original?

Teríamos que encontrar a matriz inversa de A e fazer o produto entre a mensagem cifrada e A^{-1} .

Após os devidos cálculos encontramos: $A^{-1} = \begin{bmatrix} 1 & 0 & -1 \\ -1 & 1/2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, temos então que:

$$\begin{bmatrix} 15 & 2 & 35 \\ 31 & 26 & 32 \\ 38 & 18 & 41 \\ 1 & 0 & 6 \\ 2 & 2 & 2 \\ 20 & 2 & 29 \\ 30 & 16 & 31 \\ 8 & 8 & 9 \\ 19 & 0 & 22 \\ 19 & 10 & 33 \\ 21 & 18 & 22 \\ 19 & 0 & 19 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & -1 \\ -1 & 1/2 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 13 & 1 & 20 \\ 5 & 13 & 1 \\ 20 & 9 & 3 \\ 1 & 0 & 5 \\ 0 & 1 & 0 \\ 18 & 1 & 9 \\ 14 & 8 & 1 \\ 0 & 4 & 1 \\ 19 & 0 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \\ 19 & 0 & 0 \end{bmatrix} = mensagem\ original$$

4 OFICINA DE CRIPTOGRAFIA

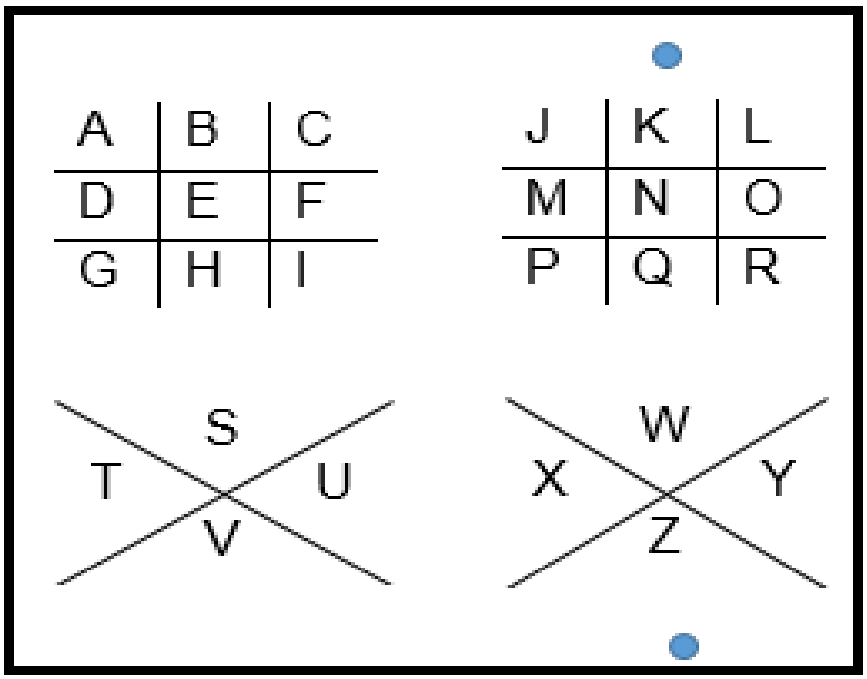
Nesta seção abordaremos como foi a oficina realizada com algumas turmas do Ensino Médio da Escola Estadual 29 de Novembro.

Inicialmente perguntamos aos alunos: vocês sabem o que é criptografia?

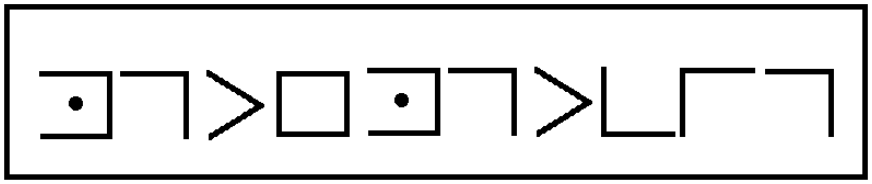
A grande maioria não tinha noção do que se tratava, e os poucos que responderam algo, fizeram sempre referência ao aplicativo de mensagens *WatsApp*, aplicativo que tem sofrido algumas sanções da justiça nos últimos meses justamente pela segurança criptográfica nas trocas de mensagens.

Em seguida repassamos aos alunos o que seria a criptografia, com conceitos, além de falarmos sobre Alan Turing e o filme ‘o Jogo da Imitação’.

Posteriormente apresentamos o alfabeto maçônico e mostramos como ele era usado.



Mostramos exemplos como seria a escrita:



Em seguida falamos da cifra de César, mostramos a forma que César se comunicava de forma secreta com seus generais, de forma a tentar ocultar as mensagens. Mostrando como faríamos para usar a cifra.

Posteriormente solicitamos que fossem formados grupos, pedimos para que os grupos se comunicassem usando a cifra de César.

Alguns tiveram um pouco de dificuldade no início da comunicação, mas foram se enquadrando junto com os colegas.

Alguns alunos mostraram na lousa como era feito o processo de descriptografia da cifra de César.

Aproveitando o bom momento de empolgação dos alunos mostramos a forma de usar o Código substituindo as letras do alfabeto pelos números de 1 a 26, como na primeira linha da tabela 1.

Na tentativa de deixar o código chave com um nível maior de dificuldade apresentamos a tabela 1, além de mencionarmos a quantidade de formas possível que poderíamos permutar as letras do alfabeto com os números de 1 a 26, porém nos restringimos nas vinte e seis permutações sequenciais apresentadas na tabela mencionada, além é claro de comentar que cada um da turma poderia criar seu próprio código.

No próximo passo conversamos sobre o conteúdo de funções que já tinha sido trabalhado em sala de aula, relembramos alguns tópicos, fazendo uma relação entre a função e a criptografia.

Foram mostrados exemplos, com algumas palavras para serem descritografadas utilizando funções como chaves e juntamente com um das linhas da tabela 1.

Sentimos a necessidade de falarmos de função inversa, mostrando o princípio, porém houve muita dificuldade por parte de alguns alunos, sendo necessário mudar a metodologia para que o conteúdo fosse mais absorvido pelos mesmo, acabamos por fim tendo que trabalhar apenas com a função fornecida na base de substituição simples.

A seguir a função e a linha utilizada para que os alunos pudessem descriptografar algumas palavras:

$$chaves\begin{cases} f(x) = 2x - 1 \\ linha\ 13\ da\ tabela\ 1 \end{cases}$$

Palavras que foram repassadas aos alunos para serem descriptografadas:

53	29	15	37	53	29	15	45	33	29

45	53	7	5	11	15	29	55	15	37

47	5	13	45	53	29	11	29		

7	29	11	29	31	37	55	13		

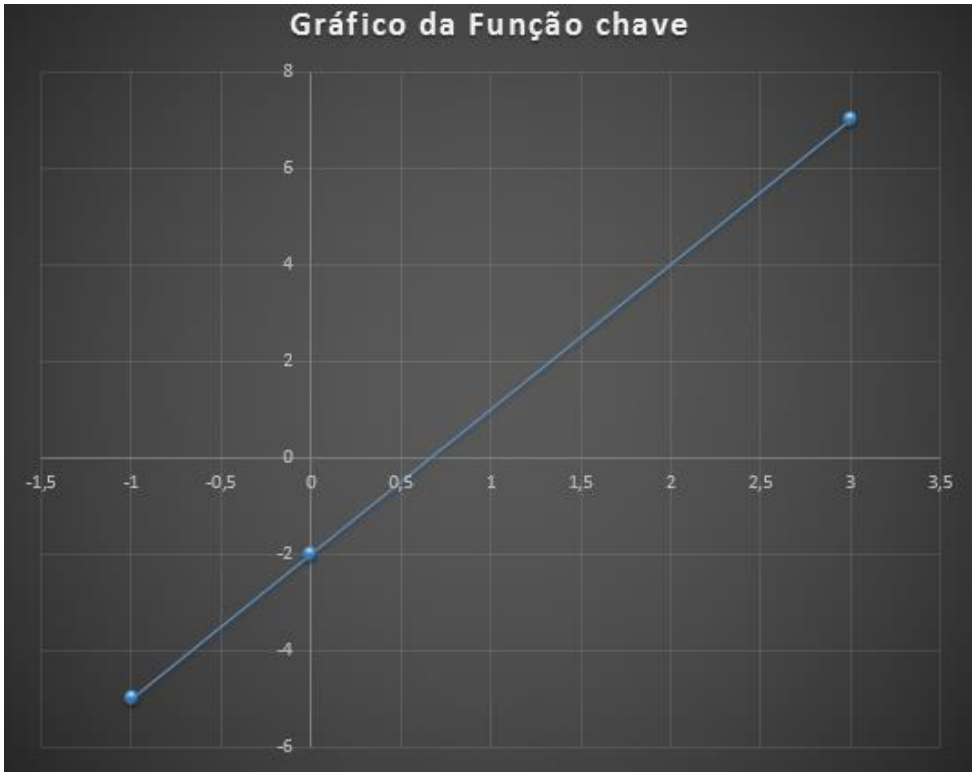
Na parte final apresentamos como desafio o seguinte texto criptografado, afim de que o os alunos fizessem o processo de descriptografia do mesmo:

7	58	7	67	28	4	0	10	49	22	25	46	52	28	1	10	0	58	0	25	46	10

64	19	46	7	55	58	0	22	58	0	22	28	46	0	31	10	7	25	46	55	58

55	58	0	31	58	7	52	58	19	0	61	10	19	0	4	46	70	10	19

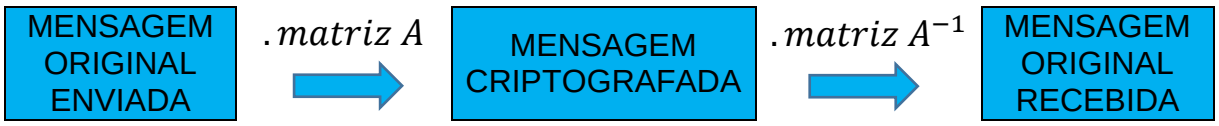
Porém ao invés de ser repassado diretamente a função, receberam a informação que a chave do enigma era função que representava o gráfico e a linha usada era o valor de x no ponto (x,46).



Dados:	
x	f(x)
-1	-5
0	-2
3	7

Resposta do Enigma: Nenhum obstáculo é tão grande se sua vontade de vencer for maior.

Em um outro momento, mostramos como o processo seria feito usando agora matrizes.



Explicamos como o que a sequência acima representava:

O texto original, é transformado em uma matriz, em seguida passa por um processo de criptografia multiplicando-se por uma matriz qualquer e não singular, ficando agora o texto cifrado, posteriormente passa pelo processo de descriptografia multiplicando-se agora pela matriz inversa da matriz escolhida anteriormente, voltando ao texto original.

Exemplos:

Linha escolhida: 5
Palavra escolhida: ENIGMAS

9	18	13	11	17	5	24

$$Matriz\ Original = MO = \begin{bmatrix} 9 & 18 & 13 \\ 11 & 17 & 5 \\ 24 & 0 & 0 \end{bmatrix}$$

Escolhemos uma Matriz qualquer:

$$Matriz\ Chave\ A = MA = \begin{bmatrix} 1 & 0 & 11 \\ -3 & 4 & 2 \\ 1 & 6 & 7 \end{bmatrix}$$

Através da multiplicação das matrizes anteriores, encontramos então o seguinte texto criptografado:

$$MO\ x\ MA \begin{bmatrix} 9 & 18 & 13 \\ 11 & 17 & 5 \\ 24 & 0 & 0 \end{bmatrix} . \begin{bmatrix} 1 & 0 & 11 \\ -3 & 4 & 2 \\ 1 & 6 & 7 \end{bmatrix} = \begin{bmatrix} -32 & 150 & 226 \\ -35 & 98 & 190 \\ 24 & 0 & 264 \end{bmatrix} = B$$

-32	150	226	-35	98	190	24	0	264

Agora para fazer o processo de descriptografia temos que multiplicar o texto cifrado pela inversa da matriz que serviu de chave, que após alguns cálculos encontramos que:

$$B^{-1} = \begin{bmatrix} -\frac{8}{113} & -\frac{33}{113} & \frac{22}{113} \\ -\frac{23}{226} & \frac{2}{113} & \frac{35}{226} \\ \frac{11}{113} & \frac{3}{113} & -\frac{2}{113} \end{bmatrix}$$

E que:

$$\begin{bmatrix} -32 & 150 & 226 \\ -35 & 98 & 190 \\ 24 & 0 & 264 \end{bmatrix} . \begin{bmatrix} -\frac{8}{113} & -\frac{33}{113} & \frac{22}{113} \\ -\frac{23}{226} & \frac{2}{113} & \frac{35}{226} \\ \frac{11}{113} & \frac{3}{113} & -\frac{2}{113} \end{bmatrix} = \begin{bmatrix} 9 & 18 & 13 \\ 11 & 17 & 5 \\ 24 & 0 & 0 \end{bmatrix}$$

Percebemos o quanto se torna complexo o processo de multiplicação e a busca pela matriz inversa, além de termos conhecimento de que temos a opção de CHAVE (escolha da matriz) infinita, fazendo com que cada grupo de aluno crie seu próprio código, por isso devido ao pouco tempo de aula, após os grupos entenderem o processo, pedimos que os alunos levassem um texto criptografado, e trouxessem no próximo encontro. Usamos o alfabeto em sua sequência normal (linha 1 tabela 1), e a matriz A como a chave das palavras

$$Matriz\ Chave\ A = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 2 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

Texto para o desafio:

7	6	12	22	8	23	2	2	2

52	30	66	22	2	26	5	0	9

5	0	27	33	28	36	41	36	41

Observação.: Cada zero encontrado no texto final é o espaço entre as palavras

5 CONSIDERAÇÕES FINAIS

Inquestionavelmente sabemos da importância da Criptografia para ‘esconder’ informações importantes. Mesmo se tratando de um assunto que aborda desde simples permutas com as letras do alfabeto, passando por números primos, divisibilidade, até a conteúdos mais avançados visto apenas em álgebra linear e teoria dos números no Ensino Superior, a forma abordada aqui com as simples aplicações podem oferecer ao leitor uma nova visão das aplicações de certos conteúdos do Ensino Básico em nosso dia a dia.

Acreditamos que professores do ensino básico possam usar este trabalho como fonte de inspiração para busca de novas aplicações dos conteúdos abordados em sala de aula, afim de tornar suas aulas mais dinâmicas, também para que aja uma busca por parte dos alunos por mais conhecimento, além é claro mostrar que sempre pode haver uma resposta boa para a pergunta: professor onde vou usar isso na vida?

Durante os trabalhos realizados em sala de aula percebemos que as aplicações de função e matrizes em criptografia foram estimulantes tanto para os alunos quanto para a professora que participou da oficina.

Durante a realização deste, percebemos o quanto podemos aplicar vários conteúdos como números primos, divisibilidade, funções (linear, segundo grau, exponencial e outros) a criptografia.

6 REFERÊNCIAS

[1] Lima, Elon Lages Lima. A Matemática do Ensino Médio – Vol. 1

[2] Beltrame, Kassia. O poder de encantar o aluno, 2015. Disponível em: <http://www.revistaeduque.com.br/noticias/o-poder-de-encantar-o-aluno/>. Acesso em: 7 de outubro de 2016.

[3] Luckesi, Cipriano Carlos. Métodos e Procedimentos de Ensino. Disponível em: <http://didaticageraluece.blogspot.com.br/ 2011/10/texto-10-metodos-e-procedimentos-de.html>. Acesso em: 7 de outubro de 2016

[4] <https://matrixcalc.org/pt/>. Acesso em: 10 de outubro de 2016

[5] Cohen, Fred. A Short History of Cryptography. Disponível em:< http://all.net/edu/curr/ip/Chap2-1.html>. Acesso em: 10 de outubro de 2016

[6] Jeffrey Hoffstein, Jill Pipher, J.H. Silverman. - An Introduction to Mathematical Cryptography 1ªEd, Springer, 2008. Disponível em: < http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.9999&rep=rep1&type=pdf>. Acesso em: 10 de outubro de 2016.

[7] Cypher research laboratories. A Brief History of Cryptography,2013. Disponível em:< http://www.cypher.com.au/crypto_history.htm>. Acesso em:13 outubro de 2016.

[8] Portal Aldeia Numaboa. As cifras hebraicas (Atbash), 2005.<http://www.numaboa.com.br/criptografia/124-substituicao-simples/168-atbash>. Acesso em: 18 de outubro de 2016.

[9] Enciclopédia Culturama. Qual é o telegrama Zimmermann?, 2015. Disponível em:<https://edukavita.blogspot.com.br/2015/03/qual-e-o-telegrama-zimmermann.html> Acesso em: 18 de outubro de 2016.

[10] Tamarozzi, Antonio Carlos. Codificando e Decifrando mensagens, RPM 45, SBM 2001.

[11] Bibliot3ca. <https://bibliot3ca.wordpress.com/o-alfabeto-maconico-mensagem-codificada-o-legado-do-quadrado-magico-do-mundo-antigo/>. Acesso em 02 de novembro de 2016.

[12] Menezes, Luiza de Abreu; Carvalho, Marcos Pavani. CRIPTOGRAFIA NA SALA DE AULA. Disponível em: <http://www.lematec.net.br/CDS/ENEM10/artigos/PT/T11_PT775.pdf> Acesso em: 18 de outubro de 2016.