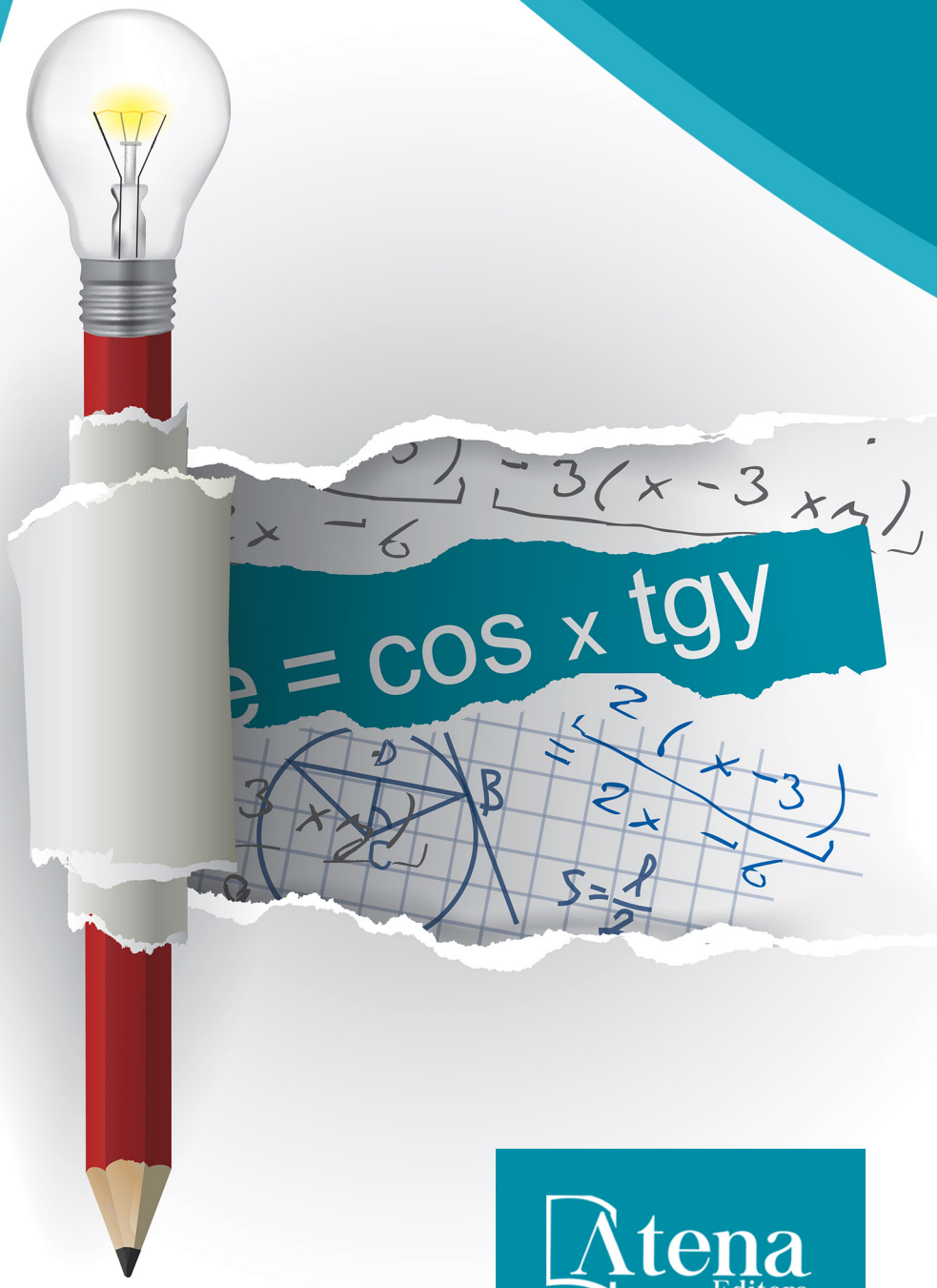
As Diversidades de Debates na Pesquisa em Matemática 3

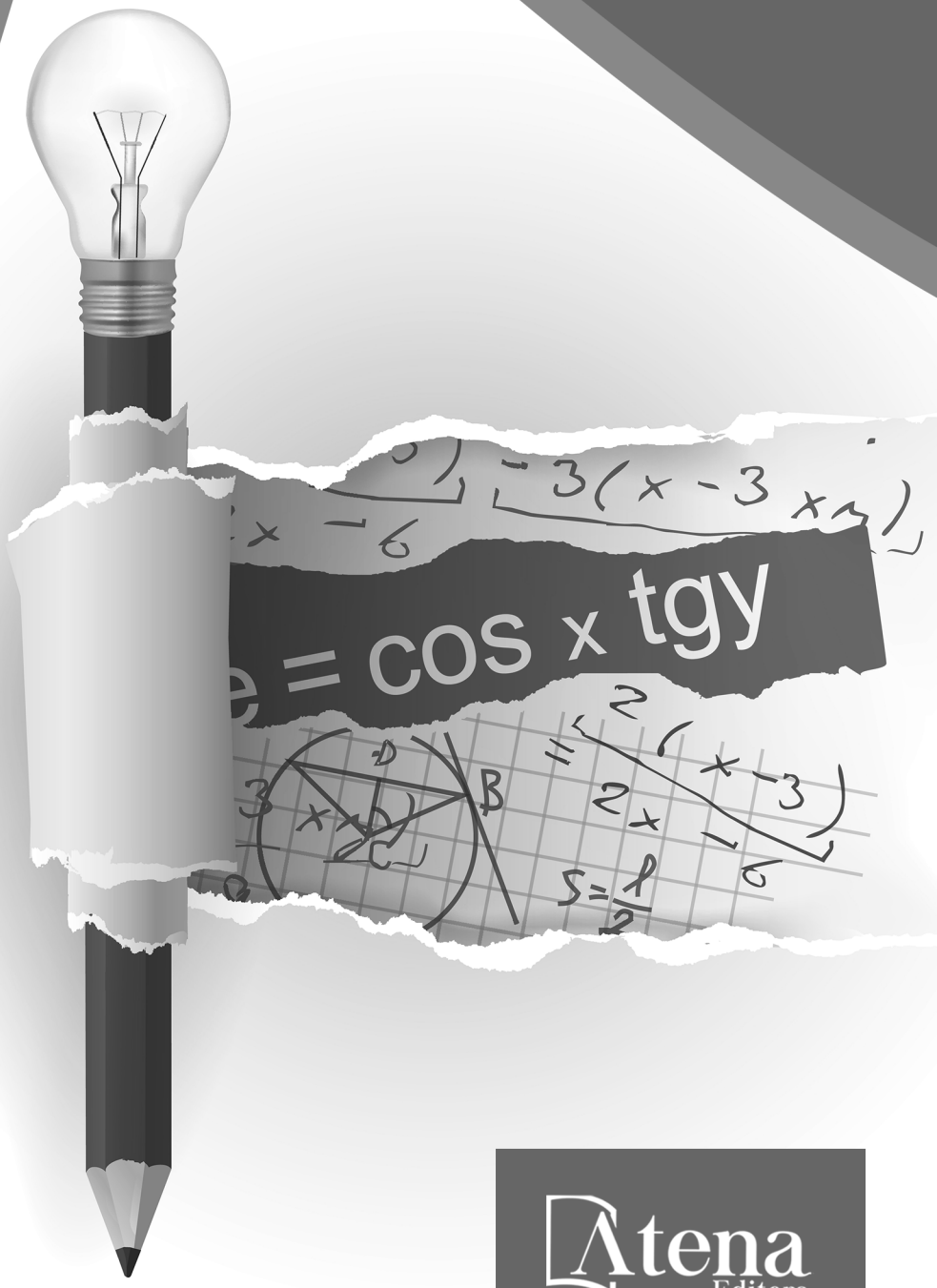
Annaly Schewtschik
(Organizadora)



Atena Editora
Ano 2020

As Diversidades de Debates na Pesquisa em Matemática 3

Annaly Schewtschik
(Organizadora)



Atena Editora
Ano 2020

2020 *by Atena Editora*

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira
Diagramação: Natália Sandrini
Edição de Arte: Lorena Prestes
Revisão: Os Autores

Atena Editora
Ano 2020

Atena Editora
Ano 2020

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

D618 As diversidades de debates na pesquisa em matemática 3 [recurso eletrônico] / Organizadora Annaly Schewtschik. – Ponta Grossa, PR: Atena Editora, 2020. – (As diversidades de debates na pesquisa em matemática; v. 3)

Formato: PDF
Requisitos de sistemas: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-85-7247-912-7
DOI 10.22533/at.ed.127201301

1. Matemática – Pesquisa – Brasil. 2. Pesquisa – Metodologia. I. Schewtschik, Annaly. II. Série.

CDD 510.7

Elaborado por Maurício Amormino Júnior – CRB6/2422

Atena Editora
Ponta Grossa – Paraná - Brasil
www.atenaeditora.com.br
contato@atenaeditora.com.br

Atena Editora
Ano 2020

APRESENTAÇÃO

A obra “As Diversidades de Debates na Pesquisa em Matemática 3” aborda uma série de livros de publicação da Atena Editora. Este Volume em seus 13 capítulos apresenta resultados de pesquisas que trazem a matemática como caminho de leitura, análise e reflexões sobre uma diversidade de temáticas da atualidade, de um ponto de vista crítico e sistemático, apresentando compreensões a partir de um diálogo da educação matemática e da matemática enquanto ciência aplicada em uso social.

Os trabalhos que evidenciam inferências frente ao campo da Educação Matemática expõem conclusões a respeito do uso de tecnologias nas aulas de matemática alavancada pelo uso de softwares educativos, o uso de jogos como uma metodológica ativa para o ensino e para a aprendizagem, incluindo neste escopo o uso de games de consoles para a aprendizagem matemática em sala de educação especial. Traz a transdisciplinaridade, fundamentada pela teoria da complexidade, como aporte para a compreensão da diversidade. Apresenta pesquisa sobre como despertar nos alunos o interesse pela estatística e a probabilidade por meio de suas diversas aplicações, assim como sobre o uso dos números racionais em atividades de compostagem para estimular consciências, ações e atitudes ecologicamente corretas.

No que tange ao uso da matemática como ferramenta para interpretações nos fenômenos sociais, apresenta pesquisas sobre o Número de Euler em constantes financeiras como ferramenta tecnológica na resolução de problemas diários, sobre as ideias de ângulos de contato em casos físico-químicos de molhabilidade na produção de tintas, sobre o uso da modelagem matemática aplicada em casos de dessalinização da água, assim como o seu uso na redução dos riscos de investimentos em pesquisa norteada pela Teoria de Carteiras. O uso de ferramentas matemáticas, como técnicas de verificação estatística também é evidenciada pelas séries temporais na pesquisa sobre modelos numéricos de previsão do tempo. E a estatística em suas séries temporais como uma ferramenta de abordagem quantitativa para questões socioeconômicas.

Este volume é direcionado para todos os pesquisadores que fazem uso da matemática como ferramenta no âmbito da ciência sociais e aplicadas, e aos educadores que pensam, refletem e analisam o ensino e a aprendizagem no âmbito da educação matemática.

Annaly Schewtschik

SUMÁRIO

CAPÍTULO 13

CRIPTOGRAFIA: O USO DA MATEMÁTICA PARA A SEGURANÇA DE INFORMAÇÕES

Data de aceite: 05/12/2018

Enoque da Silva Reis
Doutor em Educação Matemática pela Universidade Federal de Mato Grosso do Sul, Prof. do Departamento de Matemática e Estatística na Fundação Universidade Federal de Rondônia (UNIR/ campus Ji-Paraná) enoque.reis@unir.br

Marconi Limeira Gonçalves dos Santos
Graduado em Licenciatura em Matemática pela Fundação Universidade Federal de Rondônia (UNIR/ campus Ji-Paraná) Marconi.santos39@gmail.com

Jucielma Rodrigues de Lima Dias
Mestranda em Ensino de Ciências da Natureza (PGECN/UNIR campus Rolim de Moura). Graduada em Licenciatura em Matemática pela Fundação Universidade Federal de Rondônia (UNIR/ campus Ji-Paraná) jucielmarodrigues@hotmail.com

RESUMO: O objetivo deste artigo é analisar o uso da matemática para a segurança de informações, aqui em particular os elementos inerentes a criptografia. A motivação inicial parte do princípio fundamental da segurança de dados e privacidade na vida moderna, marcada pelos diversos equipamentos eletrônicos conectados à rede global de internet, onde torna-se cada vez mais necessário conhecimentos aprofundados de assuntos como o apresentado, uma vez que cada vez mais cedo inicia-se o primeiro contato de interação humana com dispositivos eletrônicos. Como referencial teórico adotado tem-se os conceitos fundamentais de Criptografia, como a cifra de Francis Bancon, Código de Morse, Código Enigma Algoritmos *Data Encryption Standard* (DES) e *Rivest-Shamir-Adleman* (RSA). Como referencial metodológico utiliza-se o método bibliográfico. Os resultados, apontam as fortes ligações existentes entre a criptografia e conteúdos matemáticos ensinados no ensino fundamental e médio, como Análise Combinatória, Estatística Básica e Funções, no entanto, a criptografia em si é pouco ou até mesmo inexplorada nestes níveis de ensino.

PALAVRAS-CHAVE: Matemática. Segurança. Criptografia.

CRIPTOGRAFIA: O USO DA MATEMÁTICA PARA A SEGURANÇA DE INFORMAÇÕES

ABSTRACT: The purpose of this paper is to analyze the use of mathematics for information security, in particular here the inherent elements of cryptography. The initial motivation is based on the fundamental principle of data security and privacy in modern life, marked by the various

electronic equipment connected to the global internet network, where it becomes increasingly necessary to have in-depth knowledge of subjects such as the one presented. earlier the first contact of human interaction with electronic devices begins. The theoretical framework adopted is the fundamental concepts of Cryptography, such as the Francis Bancon cipher, Morse Code, Code Enigma Algorithms Data Encryption Standard (DES) and Rivest-Shamir-Adleman (RSA). As methodological reference is used the bibliographic method. The results point to the strong links between cryptography and mathematical content taught in elementary and high school, such as Combinatorial Analysis, Basic Statistics and Functions, however, cryptography itself is little or even unexplored at these levels of education.
KEYWORDS: Mathematics. Safety. Encryption

1 I PRIMEIRAS PALAVRAS

A arte de interagir ou comunicar-se pode ser observado em todos os seres vivos, cada qual com suas características, sejam elas através de sons, sensibilidades, ligações químicas, dentre outros processos, simples ou complexos, mas todos com um mesmo propósito que trata de suprir a necessidade de interagir, trocar informações dentro de um contexto ao qual estejam envolvidas.

Se observarmos a história humana tendo em vista a interação entre seres da nossa espécie. Após sua descoberta na pré-história a comunicação passou a ser fundamental, dando origem, segundo historiadores, ao advento da civilização e a supremacia da raça humana. A partir disso, com a evolução da espécie também se passou a evoluir a comunicação, e assim, surgem grandes grupos vivendo em conjunto dando origem a cidades. Locais onde haviam diversas trocas de informações, vários tipos de conhecimentos e também ordens transmitidas pelos líderes a seus comandados. (EVES, 2002)

Destaca-se que nestes locais, por milhares de anos, se tem a ideia de que quanto mais eficientes a forma de comunicação, melhor controle e mais evoluída era aquela determinada civilização. Consequentemente, ao longo do tempo, foi-se tornando mais perceptível as grandes consequências sofridas se informações importantes transmitidas pelo transmissor a um determinado receptor de alguma forma fosse descoberta por uma terceira pessoa, como por exemplo, se um determinado comandante transmitisse a seu tenente informações sobre quantidade de soldados, localização de tropas ou até mesmo ordens de ataque ou recuar e seu adversário conseguisse receptar tais informações seria o fracasso da tropa. Outro exemplo pode ser observado quando tratamos de informações referentes a recursos essenciais de um uma determinada civilização, ou até mesmo informações sobre seu poder econômico, ou qualquer outra que levasse a fragilização de seu

povo, caíssem em mãos erradas.

Em registros históricos vemos inúmeras civilizações, líderes e tropas militares que sucumbiram após informações vitais terem caído em mãos inimigas, sendo assim criou-se a ideia de não somente ocultar, mas sim codificar estas informações de modo que ao se transmiti-las, somente o destinatário pudesse ler seu conteúdo, e assim possibilitando o surgimento da criptografia e a partir de então esta ciência tem como objetivo proporcionar segurança às comunicações.

Com a criação de uma forma segura de comunicação iniciou-se uma guerra que vem sendo travada até os tempos atuais, entre, os que elaboram os códigos, ou seja, criptógrafos que são os responsáveis pela garantia da segurança das comunicações, e opostos a estes, os decifradores inimigos, ou seja, são aqueles que tentam quebrar esses códigos de cifragem para ter acesso forçado, sem permissão, as informações confidencias que estejam sendo protegidas.

Ao observarmos o desenvolver desta forma de escrita protegida, pode-se notar que com o surgimento da criptografia foi implicitamente criada uma “arma intelectual” uma vez que em meio a esta guerra a segurança das comunicações está diretamente ligada à eficiência e qualidade na elaboração de uma cifragem adequada a se aplicar a informações ou dados que necessite de proteção.

Dessa forma destaca-se que este artigo tem início com alguns conceitos referentes à criptografia, em seguida, trata-se exclusivamente da evolução temporal da criptografia, ou seja, como se deu sua ascensão com o passar do tempo bem como as influências do crescimento tecnológico ligados ao processo. Posteriormente, busca-se enfatizar a ligação entre criptografia e matemática de forma a descrever os laços intrínsecos entre ambos. Seguindo, destaca-se a utilização de um sistema criptografado e sua influência no mundo tecnológico, e por fim, é realizada uma análise dos fatos históricos, relacionando a matemática e a criptografia, bem como o aspecto de utilização e relação entre esta ciência e os seres humanos.

2 I EVOLUÇÃO TEMPORAL DA CRIPTOGRAFIA

No decorrer da evolução criptográfica Singh (1999) trata sua progressão evolucional onde subdivide-se em três fases distintas e fundamentais. Devido a extensa parte histórica, nesta pesquisa, destacamos que a cada fase optamos em apresentar somente duas formas de criptografia característica dela. Basicamente sendo na primeira fase a criptografia manual, aqui exemplificada pelas formas conhecidas como Código de César e cifra de Francis Bacon. Logo após com a segunda fase, por implementação de máquinas provenientes da época ao qual temos o Código Morse e Código Enigma, e por fim na terceira fase a criptografia de uso atual com o implemento computacional, trazendo os exemplos de criptografia

por algoritmos, sendo eles o Algoritmo DES e o Algoritmo RSA.

Dessa forma, iniciamos com os primeiros relatos advindos dos egípcios onde surge a criptografia em fase manual, como anteriormente dito, o qual são sistemas clássicos e que foram utilizados até a Segunda Guerra Mundial. Pode se observar que se trata de uma forma mais rudimentar em relação às atuais uma vez que eram empregadas com uso de materiais comuns e de caráter manual. Assim temos:

2.1 O Código de Cesar

Conforme Coutinho (2009), é possível compreender que o Código de Cesar está diretamente ligado a uma forma de substituição simples, se observado nos dias atuais, mas de grande eficácia na antiguidade, com o qual se acredita que o imperador Romano Júlio Cesar[1] usufruía com frequência em suas comunicações particulares e de comandos militares. Neste código cada letra utilizada na composição das palavras em uma mensagem era substituída por uma letra três posições seguintes usando com chave o posicionamento destas no alfabeto, ou seja, a letra “A” era substituída por “D”, “B” por “E” e assim com todas as letras do alfabeto até “Z”. Assim sendo, neste sistema se cifrássemos, por exemplo, “O CODIGO DE CESAR” teríamos “R FRGLJR GH FHVDU”, lembrando ainda que o alfabeto romano possuía 26 letras e a quantia de posicionamento de referência das letras podiam ser alteradas de 3 para 4,5,6, ..., sucessivamente garantindo assim então 26 Códigos de Cesar, ou chaves de cifragem.

2.2 A Cifra de Francis Bacon

Filósofo e escritor, o Inglês Francis Bacon[2] deixou seu nome nos conceitos criptográficos com a aprimoração do sistema de substituição pela utilização do alfabeto proporcionada pela aplicação dos conceitos binários ao sistema.

Em seu método, Bacon passou a usar um alfabeto composto de 24 letras igualando a letra “I” ao “J” e “U” a “V”, com isto foi possível atribuir um grupo de 5 caracteres para cada letra do alfabeto sendo estes formados por “a” e “b”. Por serem os grupos formados por apenas duas letras caracterizou esta cifra como binária, ou seja, cada grupo possui 5 *bits* de caractere e cada caractere 2 possibilidades o que gera $2^5 = 32$ grupos permitindo representar então 32 letras diferentes.

---

1. Júlio Cesar – (100-44 a.C.) foi um político e militar romano. Além da Gália, dominou a Ásia e incorporou ao império uma vasta faixa do Norte da África. Apoiado pelo Senado tornou-se Pontífice Máximo e Ditador Perpétuo. Fonte: https://www.ebiografia.com/julio_cesar/

2. Francis Bacon nasceu em 22 de janeiro de 1561, em Londres, Inglaterra. Filho de uma família de posses, teve uma educação rara para a época. Sua mãe foi quem primeiro se ocupou de sua educação e, mais tarde, Bacon cursaria o Trinity College e, logo depois a Universidade de Cambridge indo depois para Paris. Em 1577, em Paris, Bacon iniciou sua vida política incitado pelo pai que o mandara trabalhar com um amigo, o embaixador inglês na França. A obra mais importante de Bacon, no entanto, permaneceu inacabada. Bacon morreu em 9 de abril de 1626, em Londres. (Fonte: https://www.infoescola.com/filosofos/francis-bacon/)

A formação dos grupos é uma sequência lógica onde “a” e “b” são substituídos por 0 e 1 respectivamente, compondo a cifra de tal forma:

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

Figura 01 – Grupo de letras associadas ao seu código binário criado por Bacon.

Fonte: http://numaboa.com.br/criptografia/supercifragens/331-cifra-de-bacon

Conforme apresentado, estes seriam os grupos formados pela cifra de Bacon onde ao cifrarmos, por exemplo, a palavra “BACON” teríamos “00001000000001001101011 00”, ou seja, subdividindo-se os grupos “00001/00000/00010/01101/01100” logo pela tabela temos B-A-C-O-N.

Com o avanço tecnológico e surgimento de maquinas e ferramentas que passam a auxiliar o homem em seu dia a dia tornando processos e sistemas mais sofisticados e rápidos, a comunicação criptografada, essencial desde seu surgimento, passa a acompanhar tais avanços tornando-se a cifra manual obsoleta passando-se a uma nova fase denominada de criptografia por máquinas. As tabelas, ou chaves como as já apresentadas, passaram a ser utilizadas agregadas a maquinas disponíveis na época, onde um operador de posse de uma tabela predeterminada operava a máquina com o intuito de se enviar uma mensagem criptografada.

2.3 O Código Morse

O famoso código Morse que surgiu por volta de 1840 foi um dos códigos mais utilizados durante as guerras deste período. Seu desenvolvedor, Samuel Morse[3] ao

3. Samuel Finley Breese Morse (1791-1872) nasceu em Charlestown, Massachusetts, Estados Unidos, no dia 27 de abril de 1791. Filho de um geógrafo e pastor protestante estudou no Yale College e mostrou interesse pela eletricidade e pela pintura de retratos. Em 1832, de volta à Europa, abandona a pintura e com base nas experiências do físico Michael Faraday sobre o eletromagnetismo, Morse dedicou-se ao projeto de um aparelho destinado a converter impulsos elétricos em sinais gráficos. O telégrafo elétrico e o código alfabético, usado nas transmissões telegráficas, que leva seu nome, o “Código Morse”, foi concluído em 1939. Em 1843 finalmente obtém crédito do congresso Nacional para instalar a primeira linha telegráfica entre Baltimore e Washington. (Fonte: https://www.ebiografia.com/samuel_morse/)

notar o funcionamento de uma máquina que estava se tornando promissora ao futuro das telecomunicações, o telégrafo, idealizou então transformar sinais elétricos que era como funcionava a estrutura telegráfica, em um código de comunicação que representasse mensagens, e assim o fez.

O código reconhece quatro estados de controle do telegrafo, voltagem ligada e longa representava um traço, voltagem ligada e curta um ponto, voltagem desligada e longa era espaço entre caracteres e palavras, voltagem desligada e curta espaço entre ponto e traços.

Neste código cada caractere seja ela letra, número ou sinais gráficos possuem um único conjunto de pontos e traços, onde o receptor, de posse de um manual desses sinais elétricos decifrava as mensagens que converteram as letras do alfabeto em pontos e traços. Este código é conhecido mundialmente e ainda hoje há a possibilidade de se transmitir informações a distância utilizando qualquer equipamento elétrico de transmissão sendo usado por forças militares e civis treinados em situações de perda de comunicação via rádio ou outro meio comum.

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

Figura 2 – Tabela do alfabeto aplicando o código

Fonte: https://brasilescola.uol.com.br/geografia/codigo-morse.htm

2.4 O Código Enigma

Surgindo no decorrer da Segunda Guerra Mundial, e seu título não é por acaso. O código enigma foi criado pelos alemães e superou toda tecnologia em cifras da época deixando os decifradores, matemáticos, ou qualquer um que tentasse decifrar as mensagens que eram transmitidas com o uso deste método sem sono por dias e ainda não encontravam solução.

Digna de notoriedade e fazendo jus ao nome que lhe foi conferido, a máquina enigma, intitulação esta referente ao dispositivo que proporcionava as mensagens criptografadas, compunha-se de um teclado conectado a um mecanismo codificador onde este era composto por três rotores distintos que determinavam de acordo com seus posicionamentos, como cada letra seria cifrada, sendo isto o que garantia o sucesso das cifras produzidas pela máquina, a numerosa forma de posicionamentos

e regulagens diferentes de seus rotores.

Ao se iniciar uma cifragem na máquina, os seus três rotores a serem utilizados eram escolhidos dentro de uma seleção de cinco disponíveis que poderiam ser trocados a qualquer momento para confundir eventuais decifradores espiões. Além disso, cada rotor poderia ser posicionado em vinte e seis modos diferentes e como se não bastassem às conexões do quadro de chaveamento da máquina poderiam ser mudadas manualmente. Assim com toda essa gama de opções de configurações e alterações proporcionadas pela máquina, ela oferecia um total de incríveis 150 trilhões de regulagens ou combinações possíveis. Para garantir a segurança os três rotores da máquina mudavam de orientação continuamente de modo que, a cada transmissão de uma letra alterava-se a combinação e assim o código. Por tanto se em uma palavra de uma mensagem houvesse letras que se repetissem nesta palavra, estas letras eram cifradas de modos diferentes a cada vez que surgissem.

Após o surgimento das máquinas e novas necessidades que surgiam, a evolução destes dispositivos acelerou de forma exponencial onde não podemos deixar de citar as contribuições do matemático britânico Alan Turing ao qual a este é atribuído o incrível feito de criar uma máquina ainda mais sofisticada que foi capaz de decifrar o poderoso Código Enigma do nazistas o qual acaba de ser apresentado. Revolucionando a ciência criptográfica e considerado o pai da ciência da computacional, Turing foi o percursor para que surgissem máquinas cada vez mais velozes e precisas que proporcionavam o feito de cálculos complexos serem resolvidos com mais facilidade, tornando assim um marco histórico sua atuação e contribuição na evolução bem como, sendo atribuído a ele a intitulação de criador da primeira unidade central de processamento, ou mais popular conhecido hoje como computador doméstico, o qual tomou conta desde bases governamentais e militares às residências.

A ciência avança como nunca, evoluções na física, matemática com o advento da computação gerando bilhões de cálculos por segundo em suas unidades de processamento. Surgem laptops, celulares, comunicação a longa distância, cabos de fibra ótica que transportam incontáveis dados de uma ponta a outra do planeta em um segundo, smartphones, tudo ligado a uma rede que agrega todo o planeta, uma rede onde toda e qualquer informação transferida ou guardada permite acesso de qualquer lugar, a rede de interligação global popularmente conhecida como internet.

Com toda essa evolução e necessidade de proteção de informações pessoais, militares ou de qualquer natureza, mais uma vez a criptografia molda-se pela evolução afim de garantir essa segurança e com o emprego do computador e seus algoritmos a criptografia passa a sua nova fase, a terceira e última fase, até o momento, a da criptografia em rede.

2.5 Algoritmo DES

Desenvolvido na década de 70 e conhecida como criptografia simétrica, é a forma mais convencional de criptografar dados em uma rede de acesso global. Como o sucesso da cifra é garantido pelo tamanho da chave, podendo esta ser uma palavra, frase sequência de códigos e etc, que permita de posse do algoritmo, cifrar o decifrar uma mensagem, podemos gerar chaves de 40 a 128 bits onde quanto mais bits mais fortes e seguro será a cifra. O algoritmo pode se dividir em dois modos, cifra de fluxo, que encripta um texto *bit* por *bit* ou cifra de bloco, que usa um conjunto com número fixo de *bits*, geralmente 64 *bits* nas mais modernas.

O algoritmo utiliza uma única chave secreta sendo necessário tanto o emissor quanto o receptor compartilhar entre si suas chaves secretas antes de estabelecer um canal seguro de comunicação, o que atualmente acaba sendo um problema devido ao número de pessoas conectadas comprometendo esta troca segura das chaves e como a criptografia simétrica não identifica quem enviou o recebeu a mensagem a alta quantidade de conexões de usuários na rede dificulta o gerenciamento das chaves.

Figura 3 - Exemplo de Cifragem DES

Fonte: http://www.macoratti.net/12/03/net_prot1.htm

2.6 Algoritmo RSA

Para Coutinho (2009), neste algoritmo a diferenciação em relação ao sistema DES está na assimetria. Enquanto o sistema DES elaborava criptografias simétricas, o sistema RSA as elabora de forma assimétrica denominada algoritmo de chave pública. Isto faz com que a chave possa ser de domínio público podendo ser difundida por qualquer meio de comunicação e a qualquer pessoa onde independente de uma dessas que detenham a chave disponível e acessível, possa cifrar uma mensagem, porém somente o criador da chave poderá decifrar a mensagem, pois é o único

conhecedor da chave de decodificação.

Assim tem-se nos algoritmos uma chave pública e uma privada o que garante maior segurança ao se transmitir a chave, pois servirá somente para encriptação, à chave decodificadora fica em segurança com seu real portador. É um meio encontrado para garantir a segurança de dados em uma época de livre acesso aos pacotes de informações transmitidas em meio à rede global e que explorar propriedades específicas de números primos e as dificuldades em fatoração se reduzem com uso de computadores mais potentes se torna cada vez mais rápido estas operações, no qual o Coutinho (2009, p.17) a define como:

> O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.), uma das melhores universidades americanas. As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais.

Sendo este o método de criptografia em rede de uso atual se observarmos com mais detalhes seu desenvolvimento nota-se que sua base teórica é a álgebra abstrata e a teoria dos números, dois importantes conteúdos matemáticos que proporcionam tal feito.

Não podemos deixar de observar que toda a operação é geralmente executada automaticamente por intermédio de softwares e meios de comunicação digital e para cada operação em que se emprega o uso de dados criptografados a segurança ou complexidade da criptografia pode ser menor ou maior, como por exemplo, em operações bancarias se faz necessário utilizar-se de uma encriptação muito mais complexa e segura do que a aplicada em uma troca de e-mails.

Durante os processos criptográficos aplicações matemáticas são de uso frequente, chamamos aqui a atenção que muitos desses tópicos são abordados no ensino médio, tais como, números primos, análise combinatória, aritmética modular, estatística, matrizes, funções e outras.

No processo inicial da encriptação de dados, temos primeiramente a mensagem a ser transmitida e a chave pública que é gerada por $N=P.Q$ onde p e q são primos distintos, assim para se codificar a mensagem usamos N, e para decodificá-la usamos P e Q. Ainda na pré-codificação é necessário que a mensagem seja convertida em uma sequência de números isto após a enumeração do alfabeto, depois quebrados em blocos menores que N onde nenhum bloco comece com zero ou não correspondam a nenhuma unidade linguística, assim passa-se a codificação que é feita separadamente em cada bloco.

As codificações atuais são trabalhosas e operam com números extremamente grandes graças ao auxílio da computação, o tamanho de uma chave, ou seja, N como descrito acima se recomenda para uso pessoal 768 bits o que leva a

conter aproximadamente 231 algarismos, sendo assim, precisaríamos de dois números primos, P e Q como vimos, de aproximadamente 100 e 130 algarismos respectivamente. Com tamanha complexidade e o emprego destes números imensos, mesmo com a tecnologia atual, fatorar um número de 231 algarismos e achar seus fatores primos poderia levar milhares de anos, o que torna o sistema RSA atualmente operante quando o assunto é assegurar a transmissão de informações.

Porem apenas codificar os dados não é o suficiente, pois como se trata de um sistema de chave pública, um *hacker* poderia, por exemplo, codificar uma mensagem utilizando uma chave alheia e mandar instruções ao banco para que este transfira dinheiro de uma conta a outra. Vemos então que quando o assunto é segurança de dados, os processos empregados em assegurar o sigilo são variáveis, assim, para o caso exemplificado, é necessário que o banco saiba que a mensagem foi originada por uma pessoa autorizada, ou seja, a mensagem é codificada como uma assinatura digital gerada pela chave pública junto à privada. Ilustrando, denominamos C_b e D_b as funções de Codificação e Decodificação utilizadas pelo banco e C_u e D_u as respectivas funções utilizadas por um usuário.

Sendo X um bloco de uma mensagem que o banco deseja enviar a um usuário, para o mesmo enviá-la assinada, ao invés de cifrar da forma $C_u(x)$ ele o faz através da formulação $C_u(D_b(x))$ sendo assim o banco primeiramente aplica sua chave privada e a codifica com a chave pública do usuário, para acessar a mensagem o usuário primeiramente aplica sua chave privada D_u em $C_u(D_b(x))$ que acarretará ainda na função $D_b(x)$ e depois a chave pública do banco C_b. Se a mensagem fizer sentido, torna-se claro que foi enviada pelo banco. Lembrando que as chaves C_b e C_u são as respectivas chaves públicas, logo as outras duas são privadas.

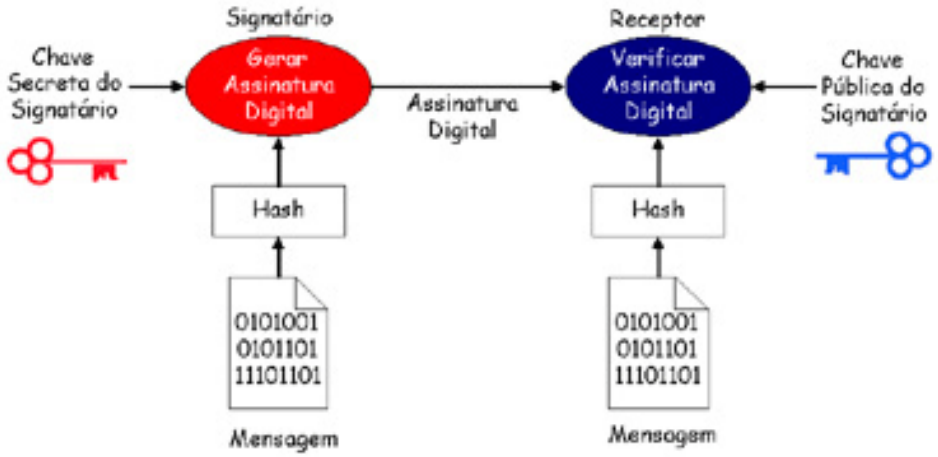


Figura 4 – Exemplo ilustrativo de como funcionam as chaves na Cifragem RSA

Fonte: http://www.lsi.usp.br/~elima/seguranca_cripto.html

3 I MOVIMENTO DE ANÁLISE

Buscamos descrever algumas relações existentes entre a criptografia e o conhecimento matemático, ou seja, se tratando de criptografar, é possível verificar nos procedimentos utilizados no processo o empenho de vários conteúdos de aplicações matemáticas, e ainda muita destas, são abordados com frequência na educação básica em nível de ensino médio, podendo ainda ser encontrado os embasamentos matemáticos em obras de autores renomados como no caso da parte algébrica por Gelson Iezzi (1992). Assim corroboramos com as palavras de Reis *et all* (2019, p.2) quando escreve que "A maioria das pessoas, quando pensam em matemática, se recordam de algo difícil e complicado de entender, e muitas dessas, desconhecem a relação existente desta disciplina com tantas outras [...]" neste caso particular, estamos observando a ligação da matemática com o fator segurança de informações.

Diante disso, passamos a de descrever algumas das aplicações da criptografia, e para finalizar, uma análise no desenvolvimento histórico desta ferramenta.

3.1 Análise Combinatória

A análise combinatória tem uma aplicação muito importante nos processos criptográficos, seu uso já se inicia na fase de pré-codificação, ela define quantas formas de alfabeto de cifras podemos ter à disposição. Em outras palavras, nada mais é do que a quantidade possível de alterações das posições da letra do alfabeto comum a fim de formar um posicionamento novo com intuito de dificultar uma decifração não autorizada.

O alfabeto cifrante precisa conter todas as letras do alfabeto original e sem repetições. Então adotando o alfabeto ocidental atual, com 26 letras, para sabermos quantas formas diferentes podemos combinar as letras usamos um cálculo matemático que é trabalhado no ensino médio, trata-se de uma permutação simples, ou seja, o número de possibilidades é de:

$P_{26} = 26!$
$P_{26} = 26 \times 25 \times 24 \times 23 \times 22 \times 21 \times \ldots \times 3 \times 2 \times 1$
$P_{26} = 403.291.461.126.605.635.584.000.000$

Figura 05 – Permutação

Fonte: Acervo do Autor

Ou seja, o valor resultante representa mais de 400 septilhões de alfabetos

possíveis, o que é notavelmente visível ser impossível humanamente se encontrar o alfabeto correto em uso checando-se as possibilidades.

3.2 Estatística Básica

Com o compreendido na obra de Coutinho (2009), na criptografia por substituição, são utilizados conceitos relativos à estatística básica. Baseado na cultura de linguagem uma simples análise estatística pode revelar características tão importantes que podem até comprometer a cifra. O exemplo disto, se tomarmos o português como a língua em uso na cifra por substituição, nesta língua assim como em outras, existe uma frequência de ocorrência de letras usadas na formação de palavras. O uso de cada letra do alfabeto em percentuais é de:

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

Figura 06- Características das repetições de letras no alfabeto português
Fonte: http://www.numaboa.com.br/criptografia/criptoanalise/310-frequencia-portugues

Sendo assim, conforme as informações apresentadas pelo criador da tabela, bem como o apresentado por Coutinho (2009), denota-se que de acordo com o autor, considerando uma característica da língua portuguesa em uso no Brasil onde o comprimento médio das palavras formadas é de aproximadamente 4.53 letras, ordenando-se então as letras por frequência de uso, e em grupos de formação temos um total de 5 vogais e acrescido a letra Y devido seu ínfimo uso no vocabulário onde juntos representam 48.75% de frequência de uso, 20 consoantes que são divididas em 3 grupos, o primeiro sendo de alta frequência de uso com 5 letras, S, R, N, D, M, com 49.12%.

O segundo grupo sendo de média frequência de uso com 10 letras, T, C, L, P, V, G, H, Q, B, F, com 21.03%. Por fim o terceiro grupo, de baixa frequência com 6 letras, Z, J, X, K, W, com 1.10%, compreendendo assim se juntarmos todos os grupos o total de 100%. Portanto, vemos que as vogais A, E, I, O, U e as consoantes S, R, N, D, M, formam mais de ¾ dos textos em língua portuguesa o que gera uma média de vogais de 4.88 para cada 10 letras.

Funções

O ato de criptografar uma mensagem ou conjunto de dados é basicamente formado por um método de transformação entre dois conjuntos, um de mensagens

escritas para o outro de mensagens codificadas, sendo está uma relação bijetora. Ao analisarmos esta pequena exemplificação do processo criptográfico torna-se perceptível a presença de aspectos matemáticos que são particulares do conteúdo de funções. Como o processo é invertível, ou seja, pelos dados resultantes do processo é possível voltar aos dados originais sendo assim, partindo da mensagem codificada podemos chegar à mensagem decodificada onde justamente se deve ter o maior cuidado na codificação que é o de esconder de forma eficiente a chave para a inversão da função de codificação. A fim de tornar mais perceptível à relação entre ambos vejamos uma exemplificação:

Primeiramente vamos enumerar o alfabeto que usamos de forma sequencial onde teremos inicialmente A = 1 sucessivamente até Z = 26. Relembrando que como visto a pouco em Análise Combinatória, é extremamente grande a quantidade de reposicionamentos que podemos formar com as letras do alfabeto e neste caso estamos utilizando-a com a organização padrão de A a Z.

Seguindo com o processo exemplificativo determinamos uma função de primeiro grau no qual irá receber os valores originais convertendo-os em valores distintos de forma a garantir o envio sem conhecimento do que se trata. Matematicamente falando, injetaremos os valores do domínio em f para que sejam transmitidos os valores da imagem de f. Por suposição usaremos a função cifradora $f(x) = 2x + 3$ e a mensagem a ser transmitida será LIMEIRA. Após a enumeração do alfabeto conforme executado no início do processo, passamos a trabalhar com os números que são relativas as letras da mensagem que iremos criptografar, assim teremos, L = 12, I = 9, M = 13, E = 5, I = 9, R = 18, A = 1, aplicando na função teremos:

Para **L** temos $f(12) = 2(12) + 3 \Rightarrow f(12) = 27$
Para **I** temos $f(9) = 2(9) + 3 \Rightarrow f(9) = 21$
Para **M** temos $f(13) = 2(13) + 3 \Rightarrow f(13) = 29$
Para **E** temos $f(5) = 2(5) + 3 \Rightarrow f(5) = 13$
Para **I** temos $f(9) = 2(9) + 3 \Rightarrow f(9) = 21$
Para **R** temos $f(18) = 2(18) + 3 \Rightarrow f(18) = 39$
Para **A** temos $f(1) = 2(1) + 3 \Rightarrow f(1) = 5$

Figura 07 - Aplicando o conhecimento de funções na escrita cifrada –

Fonte: Acervo do autor.

Após o processo de cifragem, ou seja, aplicando cada letra da palavra na função cifradora, obtivemos a sequência 27 21 29 13 21 39 5 sendo está a mensagem a

ser transmitida e que o destinatário receberá. O Receptor ao se deparar com tal mensagem verá somente uma sequência numeral aparentemente aleatória, mas que ao ser aplica em uma função inversa a que a originou, trará à tona seu real teor informativo. Para a função que utilizamos no início do processo, temos que sua inversa então seria dada por $f^{-1}(x) =$, e assim é possível através desta chave, a recuperação da mensagem contida na sequência numeral, como por exemplo:

Aplicando o valor 27 em $f^{-1}(x)$ temos $f^{-1}(27) =$, logo $f^{-1}(27) = 12$ sendo este valor o correspondente a letra **L** do alfabeto conforme enumeramos no início, e ao prosseguir com os demais valores aplicando-se a função inversa, ao fim do processo teremos novamente a palavra que ciframos anteriormente.

Como podemos notar até aqui, a relação entre a matemática e a criptografia é tão forte ao ponto de sua base de entendimento já estar presente na formação educacional em caráter inicial do homem sendo ela de forma implícita, mas com o advento da era da tecnologia podendo com certeza vir à tona já mesmo nas series inicial do aprendizado matemático.

3.3 Aplicações da Criptografia

Nos dias atuais, partindo de uma visão mais técnica do mundo tecnológico através de conceitos como os de Schneier (1996), é impossível falarmos de dados ou qualquer dispositivo eletrônico de uso pessoal ou coletivo sem mencionarmos a segurança, ou seja, sem voltarmo-nos ao assunto da criptografia.

Após a revolução tecnológica produzida pela popularização dos computadores pessoais, procedimentos e informações que antes eram manuais e mais lentos, passaram a forma digital acelerando os processos envolvidos por estes, ou seja, o que antes se demorava horas dedicadas a pilhas enormes de papeis, com o uso de um computador e pessoas qualificadas eram gastos poucos minutos, uma redução tão significativa que tomou conta rapidamente dos mais variados setores comerciais, desde o caixa de uma simples padaria aos mais avançados sistemas de grandes bancos, e não parou por ai.

Após se demonstrarem altamente eficientes para desempenhar as mais diversas tarefas do dia a dia, a tecnologia e ferramentas tecnologias como os computadores passou a se tornar além de uma ferramenta de trabalho, um equipamento pessoal e a estar presente também nas residências. Desde então sua evolução passou a ser dar de forma considerável com uma rápida expansão de empresas gigantescas do setor tais como, Microsoft, Apple, IBM, entre outras, apresentado taxas surpreendentes de aprimoramento destes aparelhos tornando-os cada vez mais potentes e menores até a chegada dos aparelhos dos dias atuais, smartphones, supercomputadores, redes sem fio, dispositivos que possibilitam

controlar tudo eletronicamente, desde monitoração de uma empresa até utensílios domésticos ou a própria residência onde hoje já são possíveis, cidades inteiras controladas por sistemas automatizados como, por exemplo, Nova York.

Porem em toda esta gama de recursos e utensílios desenvolvidos para facilitar a vida humana, e acelerar avanços também pode ser alvo de pessoas mal-intencionadas onde um banco, por exemplo, poderia por intermédio de influência externa alheia a sua vontade executar operações financeiras não autorizadas por seus respectivos clientes, através do acesso remoto de seu sistema digital. Podemos ainda citar a título exemplificativo o furto de dados pessoais de contas digitais ou dos aparelhos moveis como smartphones.

É claro o fato de que a tecnologia e os aparelhos eletrônicos foram primordiais nos avanços científicos e outros através de pesquisas, e ainda na vida particular de cada ser humano com seus benefícios, porem também é fato que toda essa gama de facilidades benéficas possa, e são usadas por pessoas mal intencionadas para proveito próprio, e assim temos a base consolidada do assunto em questão que traz a forma de segurança adequada a garantir o uso destes dispositivos, sendo assim onde ao mesmo tempo em que temos as ferramentas digitais de uso coletivo, sem esta segurança a exposição de informações seria de caráter global, ainda atualmente países altamente desenvolvidos como os Estados Unidos, Japão entre outros fazem o controle de seu poderio bélico através de sistemas informatizados via satélite, o que sem uma segurança adequada colocaria nas mãos de terceiros grande poder de fogo por controle e acesso remoto.

Todas estas exemplificações demonstram a importância e aplicação da criptografia, é ela que proporciona a segurança no tráfego de dados de um banco, ou garante a privacidade dos dados contidos em um dispositivo móvel como um smartphone, contas e cadastros virtuais, e-mails trocados ou ainda a proteção dos sistemas bélicos como supracitado.

Sua aplicação nos dias atuais é totalmente indispensável e mais ainda, é necessário uma contínua evolução de seus métodos, pois são estes que garantem a sua funcionalidade bem como também seu desenvolvimento e desempenho favorável uma vez que a evolução acelerada da tecnologia proporciona cada vez mais equipamentos e sistemas dependentes de segurança, o avanço do mundo digital e ainda a difusão destes aparelhos cada vez mais conectados à rede global de acesso à internet requer segurança cada vez mais eficaz para garantir a privacidade, ordem geral da rede, a segurança de nações, bem como o funcionamento deste complexo sistema compartilhado de informações denominado rede global.

O campo de aplicação da criptografia atualmente é vasto, sendo aumentado sua necessidade a cada nova inclusão de dados e uso de aparelhos na internet, estes são apenas alguns dos principais formas e necessidades de uso de sistemas

criptografados. Verifica-se ainda que a criptografia não é aplicada apenas quando um dado ou informação é enviado de um local a outro, ou seja, trafegando pela rede pública, ela é utilizada também em dispositivos de armazenamento de dados com os discos rígidos, pen drives, celulares modernos e dispositivos que são alvos de ataques e roubos mesmo que não virtuais.

De uma forma geral, a criptografia garante a confidencialidade da informação independentemente se esta está compartilhada em uma rede ou não.

3.4 Uma Análise dos Fatos Históricos Relacionados à Matemática e a Criptografia

De acordo com Singh (1996) e Coutinho (2009) a criptografia remonta os tempos antigos desde os grandes impérios faraônicos até os dias atuais sofrendo ao longo deste tempo modificações e melhorias, sendo aprimorada a cada nova descoberta através de pesquisas desenvolvidas para tal fim, sendo está a ideia aqui explanada, e que pudemos observar no decorrer da presente monografia, onde verificamos também com Routo (2000) que, atualmente a criptografia é fundamentalmente utilizada na internet e dispositivos a ela conectados uma vez que tornou-se grande o envio de informações através da rede mundial de computadores exigindo assim segurança no que diz respeito ao sigilo dessas informações, por muitas vezes tratar-se de informações particulares de seus usuários.

Grande parte do avanço da criptografia se deve à matemática, através dos incansáveis esforços em encontrar números primos com milhares de algarismos ou fatorar produtos tão grandes quanto estes, aprimorando cada vez mais a segurança através do grau de dificuldade alcançado nestas técnicas, pois é através deste conhecimento matemático que se estuda e traça estratégias para tornar as codificações mais complexas e difíceis de serem interpretadas por pessoas que queiram possuir informações alheias para uso indevido, atualmente no mundo virtual são os denominados “*hackers*”.

Os sistemas de segurança de bancos, lojas, sites e todos os dispositivos eletrônicos conectados à rede global utilizam a criptografia para manter sigilosas as informações de clientes e usuários.

Diferentemente dos tempos antigos, onde está ciência era utilizada principalmente como arma de guerra, com a evolução dos meios de comunicação e a interligação global por meio de rede de dados altamente avançada, possibilitada pelos avanços, tanto matemáticos bem como outras ciências exatas, podemos então dizer que atualmente temos a criptografia em seu auge, de acordo com a tecnologia disponível sendo evidentemente indispensável ao funcionamento de todo equipamento eletrônico existente com conexão global, bem como sistemas e organizações, onde a criptografia é utilizada por grandes empresas, governos e bancos, usuários comuns com seus aparelhos particulares, entre outros, ela realiza

cálculos complexos para obtenção de um modelo seguro e quase indecifrável a todo momento, sempre acompanhado as grandes evoluções da humanidade em aspectos tecnológicos, principalmente em matemática, sendo está o pilar de toda sua evolução até os tempos modernos.

Hoje imputamos o aspecto “quase indecifrável” a esta ciência devido ao fato de tornar-se de tamanha complexidade que um processo criptográfico na forma mais simples utilizada digitalmente, se tivesse que ser desenvolvida manualmente, seriam necessário milhares de anos em cálculos nessas fatorações para criptografar ou acessar uma mensagem já protegida, obviamente seria inviável ou impossível este feito. Já com o uso do computador, processadores cada vez mais evoluídos e mais rápidos, processam essas quantidades de cálculos em segundos, o que torna cada vez mais complexo o processo.

Contudo é evidente a intrínseca relação deste procedimento com os conhecimentos matemáticos em que todos têm acesso ao longo da jornada escolar, com os aspectos abordados é notório que desde os grandes impérios antigos a história nos mostra que sempre esteve presente a necessidade de privacidade em certas comunicações ou informações pessoais, e que também a cada modelo de se tornar sigiloso tais interesses, há um conhecimento matemático, lógico, que paira sobre as habilidades ou métodos empregados para o êxito ao pretendido, e que ao longo da história, evoluções, conceitos, estudos e aplicações, caminharam lado a lado com a necessidade de sigilo, particularidades pessoais, segurança, ao ponto de se tornar atualmente a ferramenta mais importante de proteção do mundo.

EM SÍNTESE

Não poderíamos deixar de enfatizar a visão obtida através de todo o caminho percorrido até este momento no que tange ao modo do ensino de conceitos matemáticos, onde persistem até os dias atuais a forma de ensino mecanizada, basicamente aplicada durante as fases iniciais na construção do conhecimento básico até mesmo em muitas matérias de nível superior, já apresentadas na faculdade.

Objetivando uma nova visão de construção de conhecimentos matemáticos, esta pesquisa bibliográfica teve como base um assunto de caráter global, concreto e de suma importância para o momento em que vivemos e cada vez mais necessário no futuro. Extraindo do tema abordado os aspectos matemáticos bem como sua relação com assuntos tecnológicos, acredito ser possível concluir que o objetivo aqui pretendido foi alcançado de forma favorável e de aplicação aceitável em uma modelagem de transmissão do conhecimento matemático uma vez apresentado as diversas características bem como conteúdos vistos durante a vida estudantil, sendo

extraídas de um assunto de cunho tecnológico, atual, e não menos importante do que se visa uma grade de ensino.

Assim sendo fato é que, a forma mecanizada do ensino matemático tem por sua caraterística o rápido esgotamento mental ou déficit de atenção uma vez que os processos repetitivos e necessários, por sua vez se tornam com o decorrer de pouco tempo monótono e cansativo, porém, seja possível contornar essa dificuldade na transmissão de conhecimentos que necessitam de sérias repetitivas para fixação através da abordagem, ou de uma modelagem que cominem assuntos atuais dos quais as aplicações necessárias possam ser extraídas e com isto criar um elo de ligação que seja capaz de prender a atenção daquele que está buscando o conhecimento, e nada melhor para isto do que a forma de aprendizado onde é possível perceber a aplicação do que está sendo aprendido.

Concluímos assim com a ideia de que este é apenas um exemplo entre milhares que se possam ser estudados ou até mesmo utilizados nos processos de ensino básico ou superior, ideias de demonstrações da utilização do conhecimento a ser adquirido no âmbito de seu dia a dia, em seu meio de convívio, uma utilização real para que possa servir como exemplo para aprender análise combinatória.

Acreditando no fator de contribuição deste trabalho para novos exemplos dentro do ensino de matemática e ainda no fato de que tal feito somente seria possível com união, respeito bem como afinco em busca de novas alternativas por todos os envolvidos no processo de ensino e ainda na aceitação de uma nova modalidade de transmissão de conhecimentos, seja ela tecnológica ou não, enfim, deixo estas palavras de Raymond Albert Kroc fundador da McDonald's Corporation, que como não poderia ser diferente do objetivo deste trabalho traz de outro contexto uma aplicação concreta para enriquecimento de tudo o que aqui foi apresentado.

Nenhum de nós é tão bom quanto todos nós, juntos. (Ray Kroc)

REFERÊNCIAS

COUTINHO, Severino; **Números inteiros e criptografia RSA**. 2. ed. Rio de Janeiro: IMPA, 2003.

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra moderna**. 2. ed. São Paulo: Atual, 1992.

EVES, H. **Introdução à história da matemática.** Campinas: Unicamp, 2002.

ROUTO, Terada. **Segurança de dados - criptografia em redes de computador**. Ed. E. Blücher, 2000.

REIS, Enoque da Silva; MENDES, Hemerson Milani ; MILANI, Samanta Margarida . **Relações Entre a Música e a Matemática: uma forma de trabalhar com frações**. *In* Ensino aprendizagem de matemática. Organizador Eliel Constantino da Silva. – Ponta Grossa (PR): Atena Editora, 2019. p. 1-13.

SCHNEIER, B.; **Applied Cryptography**. 2ª. ed. New Jersey: John Wiley and Sons, 1996.

S. SINGH. **O Livro dos Códigos.** Traduzido por A. F. Bastos. Lisboa: Temas & Debates, 1999.

S.C. COUTINHO; **Criptografia**. Ed OBEMEP, 2009.

http://www.numaboa.com.br/criptografia/criptoanalise/310-frequencia-portugues (acesso em: Terça Feira 20/02/2018 as 22:48hs)

http://www.bosontreinamentos.com.br/seguranca/criptografia-cifra-de-cesar(acesso em: quarta-feira 09/05/2018 as 22:43hs)

https://www.infoescola.com/filosofos/francis-bacon/(acesso em: 09/05/2019)

http://laumansur.pbworks.com/w/page/39729617/Quem%20inventou%20o%20c%C3%B3digo%20MORSE%20e%20como (acesso em: 09/05/2019)

http://selosdobrasil.forumeiros.com/t9545-inglaterra-2-guerra-mundial-maquina-enigma-e-a-quebra-do-seu-segredo-1941 (acesso em: 19/05/2019)

http://www.macoratti.net/12/03/net_prot1.htm (acesso em: 16/08/2019)

http://www.lsi.usp.br/~elima/seguranca_cripto.html (acesso em: 25/08/2019)

https://www.ebiografia.com/samuel_morse/ (acesso em:14/09/2019)

https://www.ebiografia.com/julio_cesar/ (acesso em: em14/09/2019)

http://www.administradores.com.br/noticias/carreira/ray-kroc-o-homem-que-fez-do-mcdonalds-a-rede-de-franquias-mais-lucrativa-do-mundo/92809/(acesso em:18/09/2019)

https://brasilescola.uol.com.br/geografia/codigo-morse.htm (acesso em: 21/09/2019)

https://www.ebiografia.com/alan_turing/ (acesso em: 19/09/2019)

SOBRE A ORGANIZADORA

ANNALY SCHEWTSCHIK - Mestre em Educação, MBA em Governança Pública e Gestão Administrativa, Especialista em Metodologia do Ensino de Matemática e Especialista em Neuropsicopedagogia, Licenciada em Matemática e Licenciada em Pedagogia. Professora da Educação Básica e do Ensino Superior em Pedagogia, Administração e Tecnólogo em Radiologia, assim como em Pós-Graduação em Educação e em Educação Matemática. Atuante na área da Educação há 25 anos, tem diversos trabalhos publicados em livros, em periódicos e em anais de eventos pelo Brasil. Atualmente é Empresária em Annaly Schewtschik Coach Educacional atuando em Consultoria e Assessoria Educacional, Avaliação e Formação de Professores, além de estar Assessora Pedagógica da Rede Municipal de Educação de Ponta Grossa – Pr.

ÍNDICE REMISSIVO

L

M

N

O

P

Q

R

S

T

U

V