CRIPTOLOGIA: POSSIBILIDADE DE ESTUDO NO ENSINO MÉDIO AMPARADA EM SUA CONCEPÇÃO HISTÓRICA

CRYPTOLOGY: STUDY POSSIBILITY IN HIGH SCHOOL SUPPORTED IN YOUR HISTORICAL CONCEPTION

***Francisco Cláudio Lima Gomes*[1]**

Instituto Federal do Tocantins

***Leniedson Guedes dos Santos*[2]**

Universidade Federal do Oeste da Bahia

***Thiago Beirigo Lopes*[3]**

Instituto Federal de Mato Grosso

Resumo

Esse trabalho traz uma discussão sobre o estudo de Criptografia no Ensino Médio, fazendo uma abordagem transdisciplinar por meio de sua historicidade. Assim, com ampla utilidade prática no cotidiano, principalmente nos aparatos tecnológicos, cria-se o questionamento sobre quais motivos levam a não se ter um estudo menos superficial de maneira transversal e interdisciplinar de Criptologia, além de raros exercícios em livros didáticos. Portanto, esse trabalho objetiva fazer uma discussão sobre a implementação da Criptologia no Ensino Médio em forma de conteúdo dentro da Matemática, explorando sua transversalidade e transdisciplinaridade possível nas outras áreas de conhecimento. Utilizando a metodologia de revisão bibliográfica e, para atingir objetivo supracitado, fazendo uma conceitualização e um breve resumo do contexto histórico destacando sua importância no desenvolvimento tecnológico. A parte histórica se faz necessária para que o estudante possa compreender que a Criptologia surge de uma necessidade e se desenvolve conforme a necessidade tecnológica. Contribuindo, desse modo, com a compreensão de alguns fundamentos científico-tecnológicos de segurança em processos de informação tão presentes em sua rotina, mesmo que não percebidas.

Palavras-chave: Criptologia. Criptografia. Ensino Médio. Transversalidade. Transdisciplinaridade.

Abstract

This work brings a discussion about the Cryptographic study in high school, making a transdisciplinary approach through its historicity. Thus, with wide practical use in everyday life, especially in technological devices, it creates the question of why it takes not to have a less superficial study of transversal and interdisciplinary way of Cryptology, and rare exercises in textbooks. Therefore, this paper aims to make a discussion on the implementation of Cryptology in high school in the form of content within mathematics, exploring its transversal and transdisciplinary possible in other areas of knowledge. Using the methodology of literature review and to achieve the

[1] Endereço eletrônico: fclgomes@yahoo.com.br
[2] Endereço eletrônico: leniedson@hotmail.com
[3] Endereço eletrônico: thiagobeirigolopes@yahoo.com.br

aforementioned goal, making a concept and a brief summary of the historical context highlighting its importance in technological development. The historical part is necessary so that the student can understand the Cryptology arises from a need and develops as technological need. Contributing thus to the understanding of some scientific and technological foundations of security in information processes so present in your routine, even if unnoticed.
Keywords: Cryptology. Encryption. High school. Transversality. Transdisciplinary..

1 Introdução

A construção e propagação do conhecimento, como meio e instrumento de acesso à cidadania, necessita de prática escolar embasada na autonomia de seus estudantes, possibilitando-lhes ter participação ativa em atividades científicas ou culturais desenvolvidas na sociedade (FREIRE, 2000). Portanto, conhecer as bases tecnológicas da produção de conhecimento é fundamental. O aparato computacional de hoje, oferece a possibilidade de explorar conteúdos matemáticos de maior complexidade e com maior aprofundamento. Por isso, há a possibilidade de alguns tópicos serem contemplados no ensino médio, entre eles destacamos Criptologia e cálculo diferencial, sendo este último defendido por Àvila (2006). A Criptologia acompanha o desenvolvimento histórico das civilizações, tendo sido crucial em guerras e, hoje, é de valor precioso para a segurança no comércio eletrônico, nos sistemas bancários, nas comunicações entre pessoas e entre governos (BURNET e PEINE, 2002). Pode-se considerar extremamente vulnerável quem dela não faz uso daí a importância de se buscar compreender seus fundamentos, sendo pessoas ou organizações.

A Lei de Diretrizes e Bases da Educação (LDB), em seu Art. 35 e inciso IV, enfatiza que uma das finalidades do ensino médio é a compreensão dos fundamentos científico tecnológicos dos procedimentos produtivos, fazendo interação entre teoria e prática, no ensino de cada disciplina. O Art. 36 destaca a educação tecnológica básica e, em seu parágrafo único, estabelece que o estudante demonstre domínio dos princípios científicos e tecnológicos que amparam a produção moderna de conhecimento das formas contemporâneas de linguagem, tudo isso ao concluir o ensino médio (BRASIL, 1996). De acordo com os Parâmetros Curriculares Nacionais (PCN), a Matemática deve ser formativa no sentido de estruturar o pensamento e o raciocínio dedutivo (BRASIL, 1997).

Complementarmente à determinação legal, existem estudos realizados por teóricos construtivistas mostrando que os adolescentes são capazes de estabelecer

hipóteses e inferir, ou seja, conseguem realizar operações mentais formais (GARDNER, 1994).

Dessa forma, é razoável e interessante que o estudante seja desafiado com atividades gradualmente mais complexas, visando seu desenvolvimento intelectual. O estudo da Criptologia, que compreende a Criptografia e Criptoanálise[4], aproxima-o de uma das bases que suportam a comunicação moderna promovida pelo avanço tecnológico e cumpre os preceitos legais das diretrizes educacionais nacionais. A Criptografia está presente em muitas atividades cotidianas, tomemos como exemplo o momento quando se usa o cartão de crédito, se faz uma transação pela internet ou em conversas de aplicativos em dispositivos portáteis.

A segurança e privacidade são cada vez mais necessárias na contemporaneidade, com isso espera-se que as mensagens eletrônicas fiquem somente entre os interessados, que as informações mercadológicas e as estratégias empresariais sejam protegidos, que os bancos transmitam a movimentação financeira sem que isso se torne público e muitos outros contextos que exigem o uso da Criptografia no cotidiano. Os governos necessitam guardar informações e mantê-las secretas. Assim percebe-se que há intensa necessidade de segurança da informação por governos, empresas, demais organizações e, por parte das pessoas, há uma grande necessidade de privacidade. A Criptografia vem em atendimento a essa demanda.

Não obstante de toda a justificativa para abordar Criptologia, existe uma lacuna que pode ser facilmente identificada. Os livros adotados no ensino médio dão pouca atenção à Criptologia, que foi fundamental durante a Segunda Guerra Mundial (COSTA, 2004).

Sendo, portanto, importante que os estudantes de ensino médio tenham contato com esse conteúdo por satisfazer as exigências legais e, devido sua transversalidade e transdisciplinaridade, possibilitar a elaboração de projetos pedagógicos interdisciplinares em que professores de diversas disciplinas, como Informática, História, Sociologia, Filosofia, Física e Matemática, possam participar e colaborar.

Assim, com toda a utilidade prática cotidiana, fica a indagação da motivação que leva a não se ter um estudo mais aprofundado de modo transversal de Criptologia, além de raros exercícios em poucos livros. Portanto, esse trabalho tem objetivo de trazer a discussão sobre a implementação da Criptologia no ensino médio em forma de conteúdo

[4] É a arte de tentar descobrir texto cifrado ou a chave de encriptação utilizada.

dentro da Matemática e explorando sua e transdisciplinaridade possível nas outras áreas de conhecimento. Contribuindo, desse modo, com a compreensão de alguns fundamentos científico-tecnológicos de segurança em processos de informação.

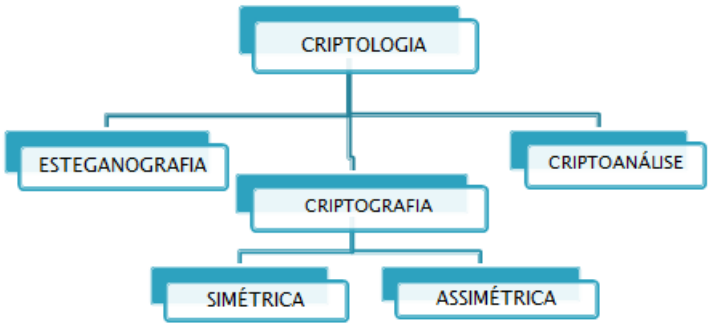
Apesar de não ter muita literatura pertinente ao tema, a metodologia utilizada foi a de revisão bibliográfica. E, para atingir objetivo supracitado, fizemos uma conceitualização em relação ao tema proposto no intuito de conceituar termos recorrente da Criptologia. Posteriormente é realizado um breve resumo do contexto histórico da Criptologia desde a antiguidade, perpassando pela Idade Média e chegando ao pós guerra. Essa parte histórica se faz necessária para que o estudante possa compreender que a Criptologia surge de uma necessidade e se desenvolve com os passar do tempo. "Nesse sentido, dentre as várias disciplinas que podem relacionar a teoria com a prática escolar é a história da matemática essa possibilidade" (PEREIRA, SILVA, *et al.*, 2016, p. 244). Também indicamos algumas possibilidades de atividades utilizando a própria História da Matemática no que concerne à Criptologia, sendo abordados os seguintes tipos de Criptografia: Bastão de Licurgo, Disco de Alberti, Tábula reta de Trithemius, Grelha de Cardano e Cifra de Vigenère.

2 Conceitos iniciais

A esteganografia consiste em esconder a existência de uma mensagem, tornando-a imperceptível às pessoas que não sejam destinatárias. Mas se a intenção for impossibilitar a leitura da mensagem por pessoas não autorizadas, alterando seus caracteres por substituição ou permutação, então faz-se o uso da Criptografia. A codificação é a alteração das características de um sinal com uma finalidade particular. Esse fim pode ser para transmissão, exibição ou arquivamento. Como exemplo, pode-se converter texto, som ou imagem para arquivá-los em dispositivos de armazenamento de dados eletrônicos. Já a cifragem é alteração de símbolos da mensagem original para torná-la acessível apenas às pessoas autorizadas (COUTO, 2008). Entende-se algoritmo como o conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas (MENEZES, 2014).

DOI: 10.30938/bocehm.v3i9.54

Figura 1 - Ramos da Criptografia



Fonte: Dos autores, baseando-se na concepção de Couto (2008).

A mensagem cifrada é fenômeno da aplicação de um algoritmo inalterável associado à uma chave específica (variável ou não). O sistema e a chave necessitam ser de conhecimento do emissor e do receptor para que se possa compor esquema com eficácia.

A Criptografia convencional é constituída principalmente por 5 elementos, que são o texto original, o algoritmo criptográfico, a chave secreta, o texto cifrado e o algoritmo de descriptografia (COUTO, 2008). O algoritmo criptográfico transforma o texto limpo em texto cifrado, a chave é um elemento peculiar para se executar tais algoritmos, o algoritmo de descriptografia converte o texto cifrado em texto limpo novamente.

Naturalmente a procura por segredos de estado, mensagens inimigas durante as guerras ou, mais recentemente, segredos industriais estimulou a procura de processos de quebra de cifras por meio da detecção da chave para um acesso não autorizado à mensagem, além do simples desafio à inteligência humana. Esse ramo denomina-se criptoanálise, que incide em um conjunto de técnicas e métodos para a decifração de caracteres de uma escrita em um sistema desconhecido (GOMES e GUIMARÃES, 2016). Mais recentemente, algumas empresas estão contratando os criptoanalistas para indicarem as fraquezas em sistemas por elas desenvolvidos.

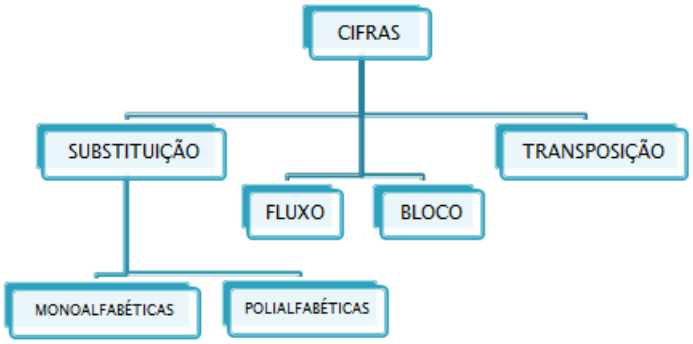
3 Cronologia da Criptologia

Considera-se como primeiro documento de escrita cifrada alguns hieróglifos egípcios, descobertos na tumba de Khnumhotep, de aproximadamente 1900 a.C. Em aproximadamente 1500 a.C. houve a evolução da esteganografia pelas culturas egípcia, chinesa, indiana e mesopotâmica. Situações como raspar o cabelo, tatuar uma mensagem, deixar o cabelo crescer, enviar ao destinatário que raspará novamente para

DOI: 10.30938/bocehm.v3i9.54

que a leitura seja efetuada é um exemplo de como a esteganografia era executada (GOMES, 2014).

Figura 2 - Classificação de cifras



Fonte: Gomes (2014, p. 19).

Segundo Couto (2008), existem inúmeros exemplos de esteganografia. Para exemplificar, há o fato de escrever um texto e ocultar a mensagem em meio ao próprio texto, realizar escritas na parte interior de caixas para transporte de cera ou, ainda, mensagens meticulosamente embaladas para serem engolidas por animais, transportada em seus estômagos e posteriormente recuperadas.

Os hebreus, entre 600 e 500 a.C., utilizaram uma cifra de permuta conhecida como Atbash, que consistia em substituir uma letra por sua simétrica em relação às extremidades do sistema alfabético utilizado. Para exemplificar, a cifra Atbash usando o alfabeto latino tem cada letra substituída pela letra diretamente embaixo, conforme a sequência mostrada no Quadro 1.

Quadro1-Atbash no alfabeto latino

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

Fonte: Dos autores.

Há indícios de que, no mesmo período, os espartanos utilizavam um bastão conhecido como Scytalae ou Bastão de Licurgo para conseguir criptografar. Esse processo consistia em envolver uma tira de couro em volta de um bastão, escrever a mensagem sobre o couro na direção do comprimento do bastão. Assim, quando desenrolado do bastão, a mensagem ficava embaralhada e necessitava que o receptor tivesse um bastão de mesmo comprimento que o utilizado pelo emissor da mensagem (COUTO, 2008).

Figura 3 - Scytalae ou Bastão de Licurgo

Fonte: Dos autores.

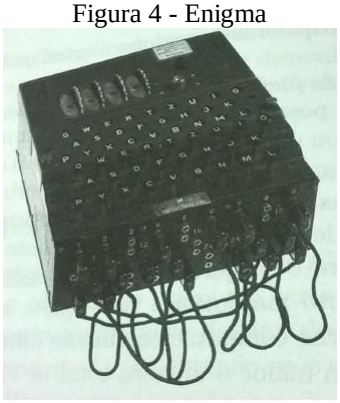
Por volta de 300 a.C., na Índia, um livro intitulado *Artha-Sastra*, possuía uma compilação de várias tecnologias e procedimentos de criptoanálise. Seu provável autor se chamava Kautilya (aprox. 300 a.C.) e tal livro era privado ao uso diplomático. O matemático grego Euclides (aprox. 300 a.C.) sintetizou o conhecimento de geometria e teoria dos números em obras aceitas como referência até hoje, *Os elementos*. O grego Erastóstenes (276 a.C.- 194 a.C.) criou um método para separar os números primos no intervalo inteiro de 1 a n, conhecido como crivo de Erastóstenes (COUTO, 2008). Os escribas de Uruk, atualmente região do Iraque, identificavam seus trabalhos transformando as letras de seus nomes em números e acrescentando a seus trabalhos, isso se dá em torno de 130 a.C. e é uma forma muito interessante de autenticação.

De acordo com Couto (2008), o general romano Júlio César (100a.C - 44a.C.) foi um dos pioneiros a utilizar em documentos oficiais uma metodologia de cifragem que consistia em trocar qualquer letrada mensagem por outras três posições à frente.

Já no século VIII, o árabe al-Khalil fica famoso no império bizantino por decifrar um criptograma antigo conjeturando que a parte inicial do texto era ‘Em nome de Deus’, então este método ficou conhecido como ‘Método da Palavra Provável’ e foi utilizado para decifrar trabalhos da máquina Enigma (Figura 4) no período da 2ªGuerra Mundial (COUTO, 2008; MOREIRA, 2015).

DOI: 10.30938/bocehm.v3i9.54

Figura 4 - Enigma



Fonte: Coutinho (2003).

Então duas inovações tecnológicas são descobertas, a primeira o árabe Al-Kindi utiliza análise de frequência para decifrar mensagens criptográficas, sendo um dos primeiros estudiosos da estatística, seu livro *RisalahfiIstikhraj al Mu'amma* é a obra sobre Criptologia mais antiga que persiste ao tempo. Já a segunda tecnologia, entre os séculos XII e XIII, o árabe Ibn Dunainir inova ao usar as cifras algébricas, que consiste em trocar letras por números e submetê-los a operações aritméticas (COUTO, 2008).

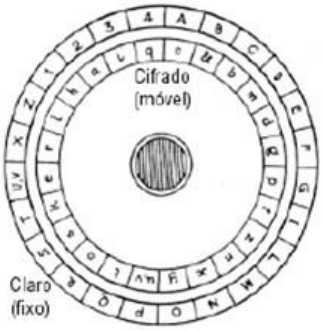
As cifras clássicas podem ser entendidas como algoritmos de transposição (permuta entre os símbolos que compõem a mensagem) ou algoritmos de substituição nos quais as letras são trocadas por outras letras ou símbolos (permuta entre os símbolos que não precisam necessariamente compor a mensagem).

Na cifra de colunas a mensagem há a distribuição, de cima para baixo, em uma grade que depois é quebrada em blocos de k termos da esquerda para a direita. Faz-se necessário o conhecimento do tamanho da tabela e da chave para se descriptar. Há também a transposição de colunas, onde o texto encriptado consiste na sequência formada pelas colunas, em ordem alfabética das letras da palavra-chave (COUTO, 2008).

Segundo Pantoja (2013), por volta de 1467o arquiteto italiano Leon Battista Alberti (1404 - 1472) inventou e publicou a primeira cifra polialfabética e também cria um disco para facilitar a cifragem que fica conhecido como Disco de Alberti, por esse motivo Alberti é considerado o pai da Criptologia ocidental. Desse modo se dificultava o uso da análise de frequência para descriptação de textos. O disco de Alberti era composto por dois discos concêntricos divididos em 24 partes igualmente espaçadas conforme a **Erro! Fonte de referência não encontrada.**.

DOI: 10.30938/bocehm.v3i9.54

Figura 5 - Disco de Alberti



Fonte: http://www.dm.ufscar.br/~caetano/iae2004/G6/disco.htm

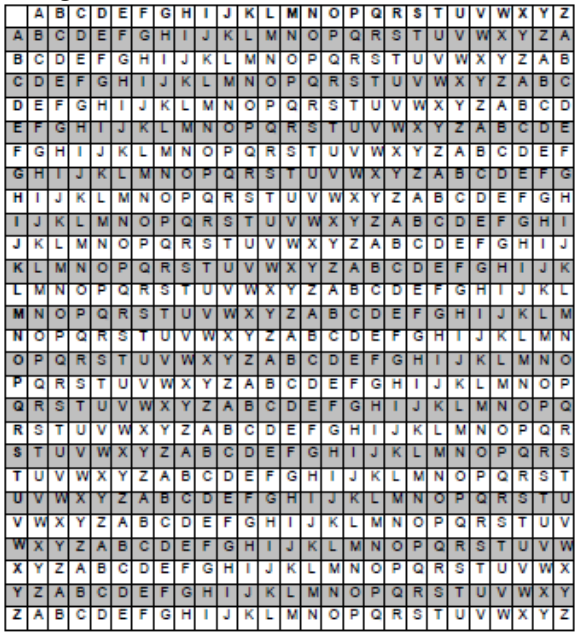
Internamente, um disco fixo apresenta-se o alfabeto latino ordenado com 20 letras (suprimidas h, j, k, w e y), no outro externo, que pode girar, o alfabeto latino sortidamente distribuído e os números de 1 a 4. Naturalmente, era preciso que o destinatário tivesse em posse um disco idêntico e conhecesse uma determinada letra chave (COUTO, 2008).

A Grelha de Cardano, idealizada pelo italiano Girolamo Cardano (1501 - 1576), consiste em uma página de material rígido onde há aberturas retangulares da altura de uma linha de texto e o comprimento podendo ser variável, colocadas em intervalos aleatórios. O remetente sobrepõe esta matriz sobre a página de papel e escreve a mensagem nas lacunas a mensagem a ser escondida. Posteriormente retira a grelha e preenche os espaços em branco com letras quaisquer. O destinatário meramente coloca uma grelha idêntica sobre a página recebida para fazer aparecer a mensagem(CASIERRA, 2009).

Em 1518 foi escrito o que é considerado o primeiro livro impresso sobre Criptologia pelo alemão Johannes Trithemius (1462 - 1516) que também inventou uma cifra esteganográfica. No final do século XIV ele criou uma tabela, conhecida como Tábula Reta de Trithemius (Figura 6), para cifras poli alfabéticas análogas às de Alberti (MARTINS, 2005). Para cifrar usando a tabela reta, mantém-se a primeira letra da mensagem, a segunda letra é trocada pela letra imediatamente da segunda linha, a terceira letra da mensagem deve ser trocada por letra da terceira linha pertencente à mesma coluna da substituída e assim em diante (COUTO, 2008). Por exemplo, a palavra TOCANTINS é cifrada torna-se TPEDRYOUA. Bastando subir as letras para retornar á palavra inicial.

DOI: 10.30938/bocehm.v3i9.54

Figura 6-Modelo de Tábula Reta de Trithemius



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

Fonte: Dos autores.

Giovan Batista Belaso (1505 - ?), usando uma tabela análoga, estabelece um método conhecido como cifra de Vigenère em 1553 (MARTINS, 2005). Os deslocamentos na cifra de Vigenère estão relacionados à uma chave. Escolhida a chave o processo de cifragem consiste em trocar uma letra por outra pertencente à mesma coluna. A sequência de letras da palavra-chave articula, respectivamente, em que linha procurar a letra substituta (GOMES, 2014). Exemplificando, escolhe-se a chave: GRITO, deve-se buscar a substituta para a primeira letra do texto inicial na intersecção de sua própria coluna com a linha iniciada por G; deve-se trocar a segunda letra do texto inicial na coluna em que ela se encontra intersecção com a linha iniciada pela letra R e assim sucessivamente. Após o uso da última letra da chave, novamente executa-se processo a partir da primeira letra que, no caso, é a letra G (COUTO, 2008). Como exemplo será cifrando: MATEMATICA usando a chave GRITO.

Usando a Tábula Reta da Figura 6, a primeira busca é realizada na primeira linha, então busca-se o M e desce por sua coluna, que é a 14ª, até a linha iniciada por G, que é a 8ª e que é a primeira letra que pertence à palavra-chave, encontra-se a letra T nesta intersecção. Assim a letra M será substituída por T. Localiza-se na primeira linha da Tábula Reta, a segunda letra a ser substituída, letra A. Sua substituta está na mesma coluna da letra A (2ª coluna) na linha iniciada pela letra R (19ª linha), a intersecção da 2ª coluna com a 19ª linha representa a letra S, logo a letra A é substituída por S. Sendo a palavra-chave utilizada de forma cíclica como já foi mencionado.

Tabela 2 - Cifra de Vegenère

Texto	M	A	T	E	M	A	T	I	C	A
Chave	G	R	I	T	O	G	R	I	T	O
Cifra	T	S	C	Y	B	H	L	R	W	P

Fonte: Dos autores.

Um sistema de chave dupla foi criado por Giam Battista Della Porta (1535 - 1615) em 1563. A cifra é constituída de 11 alfabetos, conforme Figura 7, em que as letras de uma mesma coluna são cambiáveis na cifragem (JÚNIOR, 2015).

Uma palavra-chave era utilizada e determinava o uso dos alfabetos. Gomes (2014) estabelece a seguinte exemplificação, será usada a palavra-chave NATO, para cifrar o texto ENSINO MÉDIO. Localiza-se o alfabeto que possua a letra N. Esse alfabeto é MN, conforme Figura 7, nele as letras E e Y se encontram na mesma coluna e, devido a isso, o E deve ser trocado por Y. Em seguida procura-se o alfabeto que possua a letra A. Esse alfabeto é AB e nele N e A estão dispostos na mesma coluna, o N é trocado por A. Para encontrar o substituto de S procura-se um alfabeto que tenha a letra T que é o ST e, nele, a letra S deve ser substituída por B e assim continuamente. A chave também é utilizada de modo cíclico, ou seja, ao se usar a última letra volta-se a usar a primeira e a segunda, e assim sucessivamente. O resultado é a cifra YABOGB QWXVK.

Figura 7 - Modelo do alfabeto Della Porta

Alfabeto	Letras intercambiáveis												
AB	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
CD	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
GH	A	B	C	D	E	F	G	H	I	J	K	L	M
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
IJ	A	B	C	D	E	F	G	H	I	J	K	L	M
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
KL	A	B	C	D	E	F	G	H	I	J	K	L	M
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
MN	A	B	C	D	E	F	G	H	I	J	K	L	M
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
OP	A	B	C	D	E	F	G	H	I	J	K	L	M
	T	U	V	X	W	Y	Z	N	O	P	Q	R	S
QR	A	B	C	D	E	F	G	H	I	J	K	L	M
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
ST	A	B	C	D	E	F	G	H	I	J	K	L	M
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
UV	A	B	C	D	E	F	G	H	I	J	K	L	M
	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
WX	A	B	C	D	E	F	G	H	I	J	K	L	M
	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
YZ	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	N

Fonte: Dos autores.

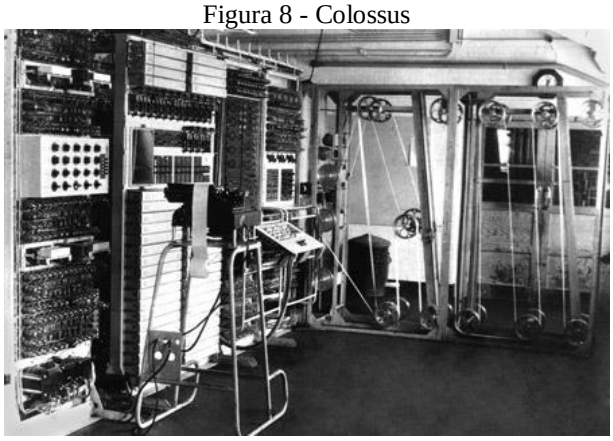
Durante o século XX, italiano Guglielmo Marconi (1874 - 1937) patenteia o rádio em 1901 iniciando a comunicação à distância e sem fio (COUTO, 2008). Em 1917

o norte americano Gilbert Sandford Vernam (1890 - 1960) cria uma máquina de encriptar polialfabética que usa uma chave totalmente randômica. Em 1919 uma máquina cifrante com base em rotores é patenteada pelo holandês Hugo Alexander Koch (1870 - 1928) que repassa sua criação a Arthur Scherbius, empresário que fabrica e vende ao exército alemão a máquina que fica conhecida como Enigma (LIMA, 2013).

Em 1929, o estadunidense Lester S. Hill (1891 - 1961) mostra um método de cifragem embasado no uso de operações matriciais, esse método ficou conhecido como Cifra de Hill. Um ano depois, em1930, William Friedman (1891 - 1969) inventa a máquina Sigaba, conhecida também como Conversor M-134. Para comparação, enquanto a máquina Enigmaera constituída de 4 ou 5 rotores, o M-134 era constituída de 15 rotores, sendo 10 para transformação de caracteres e 5 para controle de passos (COUTO, 2008).

Os japoneses apresentaram, em 1937, a máquina Púrpura. Esta utilizava relês telefônicos em substituição aos então tradicionais rotores e isso ampliava a quantidade de permutações a cada passo (COUTO, 2008). Em 1943 os ingleses põem em ação a partir do Centro de Estudos Criptológicos da Inglaterra, situado em Bletchley Park, um computador para analisar e quebrar códigos, chamado Colossus (OLGIN e GROENWALD, 2011).

Figura 8 - Colossus



Fonte: http://www.colossus-computer.com/colossus1.html

Segundo Couto (2008), na década de 60 o alemão Horst Feistel (1915 - 1990), líder de um grupo de pesquisa da International Business Machines (IBM), apresenta a cifra denominada Lucifer, uma cifra de bloco onde a versão DTD-1 começa a ser utilizada nos caixas eletrônicos dos bancos nos anos 70. O governo americano faz uma análise da cifra Lucifer em 1976, com o auxílio das National Secutity Agency (NSA) e National Bureau of Standards (NBS), sugerindo algumas alterações e começam a

utilizá-la como padrão de encriptação conhecida como Data Encryptation Standard (DES).

Durante muito tempo, a Criptografia foi realizada com o uso de chaves simétricas, que é a utilização da mesma chave para cifrar e decifrar. O que, de certa forma, é uma limitação, pois há dificuldade no modo de comunicar essa chave entre os envolvidos ou no gerenciamento de múltiplas chaves em comunicação com uma quantidade elevada de pessoas.

Bailey Whitfild Diffie (1944 -) e Martin Eduward Hellman (1945 -) fazem a sugestão do uso de chave pública, baseada em uma função de via única, publicado no artigo intitulado *New Directions in Cryptography*, no volume 22 da revista IEEE Transactionson Information Theory (FALEIROS, 2011). Na Criptografia, a essência das chaves começa a ser vislumbrada de dois modos, podendo ser simétricas ou assimétricas. A utilização de chaves assimétricas, em que o emissário e o receptor da mensagem possuem chaves forma inversa à outra, resolveu os entraves de distribuição e gerenciamento de chaves.

Os pesquisadores Ronald L. Rivest (1947 -), Adi Shamir (1952 -) e Leonard M. Adleman (1945 -) acatam a sugestão de Diffie e Hellman e apresentam a cifra RSA (letra inicial de cada pesquisador), uma cifra de chave pública, que se consistia em tanto em um processo de Criptografia quanto para Assinatura Digital (COUTO, 2008).

Antes do século XX a criptoanálise podia ser tentada com papel e caneta, mas as inovações como as máquinas baseadas em rotores durante as grandes guerras mundiais tornaram essa tarefa extremamente complicada. Ainda assim foi possível ao gênio de Alan Turing e sua equipe, cujo trabalho assentou as bases para a computação. O computador pode efetuar uma quantidade de cálculos que é impossível de realizar à mão por uma pessoa. As mensagens são convertidas em bits, que é a base na linguagem de computadores, e então são encriptadas. Podendo este trabalho ser realizado pelo algoritmo de fluxo ou de bloco. O algoritmo de fluxo executa bit a bit a mensagem inicial, alguns algoritmos de fluxo são o RC4 e one-time-pad, sendo este último considerado como o único matematicamente inquebrável por ter a chave na mesma dimensão da mensagem. Já o algoritmo de blocos, unifica em um ‘pacote’ de bits e encripta todo o bloco de uma única vez, alguns exemplares são o DES, IDEA E RC5 (CARVALHO, 2000).

Cada bit pode adquirir um em dois valores, 0 ou 1, e cada vez que se aumenta um bit duplica-se a quantidade de combinações possíveis naquele espaço. Por exemplo, uma chave de 10 bits é 2^{10}, que equivale a 1024 possibilidade. Já se utilizarmos uma chave de 64 bits será, número de chaves possíveis subirá para aproximadamente 2^{64}, um número grande até mesmo para um computador.

Em 1990, de acordo com Couto (2008), são divulgadas as primeiras experimentações em Criptografia Quântica, baseadas no artigo precursor do estadunidense Charles H. Bennett (1943 -) em 1984 e do canadense Gilles Brassard (1955 -). Em 1999 o padrão DES de 56 bits foi, não sendo a primeira vez, quebrado por um computador chamado Deep Crack após trabalhar durante 22 horas e 15 minutos. Em consequência, o governo americano adota o triple-DES, a aplicação tripla do algoritmo DES com chaves de 64 bits. No ano 2000 o DES é substituído pelo Advanced Encryption Satandar (AES), que antes era denominado de algoritmo Rijndael (COUTO, 2008).

4 Considerações Finais

A Criptografia é um tema que abrange assuntos atuais, sendo bastante difundida no processo de segurança em comunicação. Mesmo assim este assunto é pouco conhecido para os estudantes do Ensino Médio, portanto propomos um estudo acerca da Criptografia utilizando sua importância e desenvolvimento históricos, abordando sua característica transversal dentro da Matemática e interdisciplinar. Contribuindo, desse modo, com a compreensão de alguns fundamentos científico-tecnológicos de segurança em processos de informação.

Buscando ainda neste trabalho, apresentar a Criptografia, no Ensino Médio por ser um tema integrante do cotidiano e, mesmo assim, poucos têm conhecimento sobre esses procedimentos, pouco se discutindo sobre a Criptografia, essa que tem possibilitado o comércio eletrônico, as comunicações e, de certa forma, a dinâmica de informação mundo nas últimas décadas.

Entre as possibilidades de atividades, há de se realizar um trabalho integrador com outras disciplinas, como Física, Matemática, História, Filosofa e Informática, em que se possa fazer uma reflexão sobre necessidades contemporâneas próprias como segurança, privacidade, cidadania, direito à informação, direito à expressão e à participação na construção de uma cidadania global que se indica. Também apontamos

DOI: 10.30938/bocehm.v3i9.54

algumas possibilidades de atividades utilizando a própria História da Matemática no que concerne à Criptologia, sendo abordados as seguintes ferramentas de Criptografia: Bastão de Licurgo, Disco de Alberti, Tábula reta de Trithemius, Grelha de Cardano e Cifra de Vigenère.

Portanto proporcionamos um material sobre o a história da Criptologia e a possibilidade de atividades embasadas em instrumentos históricos para os em estudar ou abordar esse tema no Ensino Médio. É frustrante perceber que a exploração do potencial computacional em sala de aula ainda é pouca. Onde o estudante não sai com formação para se transformar de agente passivo usuário de tecnologias e equipamentos para agente ativo no desenvolvimento das mesmas.

Referências

ÀVILA, G. Limites e derivadas no Ensino Médio? **Revista do Professor de Matemática**, São Paulo, n. 60, 2006. 30-38.

BRASIL. **Lei número 9394, 20 de dezembro de 1996:** Lei de Diretrizes e Bases da Educação Nacional. Brasília: Planalto, 1996. Disponivel em: <http://www.planalto.gov.br/ccivil_03/leis/L9394.htm>. Acesso em: 10 Junho 2016.

BRASIL. **Parâmetros curriculares nacionais:** matemática. Brasília: MEC/SEF, v. 3, 1997. 142 p.

BURNET, S.; PEINE, S. **Criptografia e Segurança:** o guia oficial do RSA. Tradução de Edson Fumankiewicz. Rio de Janeiro: Elsevier, 2002.

CARVALHO, D. B. D. **Segurança de dados com Criptografia:** métodos e algorítmos. Rio de Janeiro: Book Express, 2000.

CASIERRA, J. P. C. **Implementação de um sistema esteganográfico para inserção de textos em sinais de áudio**. Recife: Dissertações de Mestrado em Engenharia Elétrica - Universidade Federal de Pernambuco (UFPE), 2009.

COSTA, R. D. Sociedade de controle. **São Paulo em perspectiva**, São Paulo, v. 18, n. 1, 2004. 161-167.

COUTO, S. P. **Códigos & Cifras:** da antiguidades à Era Moderna. Rio de Janeiro: Nova Terra, 2008.

FALEIROS, A. C. **Criptografia**. São Carlos: SBMAC, 2011.

FREIRE, P. **Pedagogia da autonomia:** saberes necessários à prática educativa. 15ª. ed. São Paulo: Paz e Terra, 2000.

GARDNER, H. **Estruturas da mente:** a teoria das inteligências múltiplas. Tradução de Maria Adriana Veríssimo Veronese. Porto Alegre: Artes Médicas, 1994.

GOMES, F. C. L. **Uma proposta de abordagem no Ensino Médio da Criptografia RSA e sua estrutura matemática**. Gurupi: Dissertação de Mestrado Prossional em Matemática - Universidade Federal do Tocantins (UFT), 2014.

GOMES, O. S. M.; GUIMARÃES, R. L. M. Projeto e desenvolvimento de um hardware reconfigurável de criptografia para a transmissão segura de dados. **ForScience**, Formiga, v. 2, n. 2, 2016. 01-06.

JÚNIOR, F. D. P. S. D. M. A Magia Naturalis de Giambattista Della Porta: segredo e comunicação secreta na obra do poeta napolitano. **Outras Fronteiras**, Cuiabá, v. 2, n. 1, 2015. 01-18.

LIMA, K. C. S. A. D. **Números Primos e Criptografia:** Da Relação com a Educação ao Sistema RSA. Seropédica: Dissertação de Mestrado Prossional em Matemática - Universidade Federal Rural do Rio de Janeiro (UFRRJ), 2013.

MARTINS, A. M. D. G. C. **Elementos de Criptologia:** uma aplicação da Álgebra. Lisboa: Dissertação de Mestrado em Matemática - Universidade do Minho (UM), 2005.

MENEZES, A. M. D. **Os paradigmas de aprendizagem de algoritmo computacional**. Lisboa: Dissertação de Mestrado em Ciências da Educação - Universidade Lusófona de Humanidades e Tecnologia (ULHT), 2014.

MOREIRA, C. B. **Gestão da informação**. Curitiba: Gráfica Unicentro, 2015.

OLGIN, C. D. A.; GROENWALD, C. L. D. O. Engenharia Didática: uma experiência com o tema Criptografia. **Jornal Internacional de Estudos em Educação Matemática**, v. 4, n. 2, 2011.

PANTOJA, C. E. Recomendação para uso do teste de frequência Monobit do NIST em sistemas criptográfico. **Revista Tecnologia & Cultura**, Rio de Janeiro, v. 21, n. 15, 2013. 57-65.

PEREIRA, A. C. C. et al. Sobre o uso de fontes na disciplina de História da Matemática: Problema 56 do Papiro de Rhind. **Revemat: Revista Eletrônica de Educação Matemática**, Florianópolis, v. 10, n. 2, 2016. 243-257.