CRIPTOGRAFIA: EVOLUÇÃO HISTÓRICA E APLICAÇÃO NA FUNÇÃO AFIM E SUA INVERSA

Ramon Chagas Santos[1]

Karina França Bragança[2]

Silvana Leal da Silva[3]

Lívia Azelman de Faria Abreu[4]

Educação Matemática no Ensino Médio

Resumo: Este minicurso foi desenvolvido como parte de um Trabalho de Conclusão de Curso da Licenciatura em Matemática do Instituto Federal Fluminense e tem como objetivo apresentar a Criptografia como ferramenta no estudo de função afim e de sua inversa. Esta pesquisa foi motivada pelo desejo de trabalhar um tema atual, dinâmico e presente no cotidiano dos educandos. A Criptografia, além de ser um tema presente na atualidade, apoia-se na matemática para assegurar o sigilo necessário na comunicação. Para tanto, pretende-se trabalhar com alunos que já tenham estudado função afim e sua inversa, pois o intuito não é ensinar o conteúdo e sim trazer significado por meio da Criptografia. Essa proposta será iniciada com uma apresentação da evolução histórica da Criptografia, utilizando vídeos, trechos de filmes, apresentação oral e exemplos práticos. Em seguida, a ideia é realizar uma gincana com atividades que possibilitarão aos alunos a capacidade de cifrar e decifrar mensagens, além de utilizar outros mecanismos tais como a esteganografia, análise de frequência e teste de força bruta. Após esse momento de contextualização do tema, os participantes serão incentivados a utilizar a função afim como ferramenta para cifragem de mensagens e a função inversa da função afim no processo de decifragem. Espera-se com essa atividade, promover um estudo sobre Criptografia e suas aplicações na Matemática e no cotidiano, além de possibilitar que a aprendizagem de função afim e de sua inversa seja significativa.
Palavras Chaves: Criptografia. Função Afim. Função Inversa.

1. INTRODUÇÃO

A importância de buscar-se métodos dinâmicos e temas atuais no processo de ensino e aprendizagem é mencionada nos Parâmetros Curriculares Nacionais do Ensino Médio – PCNEM (BRASIL, 2002). Este documento destaca a necessidade da educação se voltar para o desenvolvimento das capacidades de comunicação, de resolver problemas, aperfeiçoar conhecimentos e valores, visto que a sociedade está integrada a uma rede de informação crescentemente globalizada (BRASIL, 2002).

Mais especificamente, a função da Matemática segundo os PCNEM (BRASIL, 2002) é, e necessita ser, mais do que memorizar resultados oriundos dessa ciência.

[1] Licenciando em Matemática. IFFluminense. ramonchagassantos@hotmail.com

[2] Licencianda em Matemática. IFFluminense. karinabraganca14@gmail.com

[3] Licencianda em Matemática. IFFluminense. silva.sleal@gmail.com

[4] Mestrado Profissional em Matemática. IFFluminense. livia.abreu@iff.edu.br

A obtenção do conhecimento matemático, precisa estar vinculada ao domínio de um saber fazer Matemática e de um saber pensar matemático (BRASIL, 2002).

Além disso, destaca-se a importância da contextualização e interdisciplinaridade, ou seja, permitir conexões entre diversos conceitos matemáticos e aplicações dentro ou fora da Matemática, conforme afirmado pelos PCNEM (BRASIL, 2002).

Nesse sentido, Pereira, V. (2012) considera a Criptografia uma temática com potencial didático para contextualização de conteúdos matemáticos. Este tema apresenta material útil para a compreensão de importantes conceitos matemáticos, podendo tornar as aulas de Matemática dinâmicas e motivadoras (PEREIRA, V., 2012).

Acerca do tema Criptografia, Pereira, N. (2015) afirma que:

> Muitos conceitos matemáticos utilizados em Criptografia fazem parte da grade curricular do Ensino de Matemática. Dessa forma, associar os conceitos a uma aplicação tão corrente nos dias de hoje, torna a aprendizagem mais significativa (PEREIRA, N., 2015, p.6).

Alguns desses conceitos matemáticos utilizados na Criptografia, de acordo com Santos (2013) e Borges (2008) são os de funções, matrizes, análise combinatória, teoria dos números e geometria analítica.

Dentre esses conceitos, optou-se por desenvolver neste trabalho o tema funções e, mais especificamente, função afim e sua inversa, primeiro porque de acordo com os PCNEM (BRASIL, 2002), o ensino isolado deste tema não permite a exploração do caráter integrador que este possui, e segundo, pelo fato da função afim ser invertível. Esta característica é a garantia do processo de codificação de mensagens ser reversível e suas informações poderem ser reveladas pelos receptores (TAMAROZZI, 2001).

Aspectos relevantes da história da Criptografia

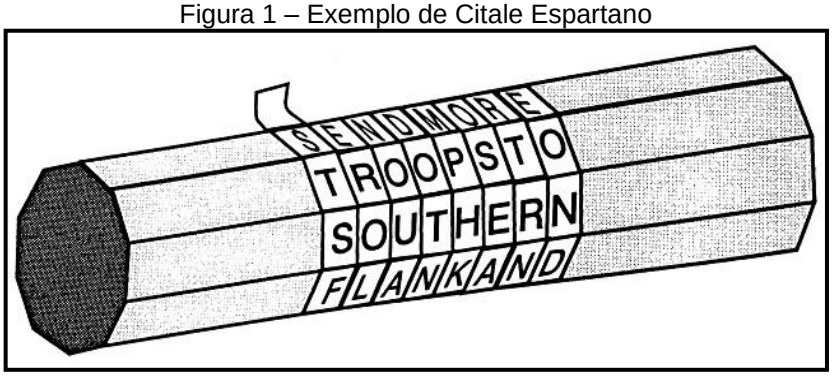
Segundo Tamarozzi (2001), Criptografia é uma palavra que vem do grego kryptós, de “oculto” e gráphein de “escrita”. A Criptografia utiliza métodos para transformar uma mensagem em um código, por meio de recursos matemáticos, de modo que apenas o seu destinatário legítimo consiga interpretá-lo.

Toda parte histórica, apresentada nessa subseção, baseia-se na obra “O livro dos códigos: A ciência do sigilo – do antigo Egito à criptografia quântica”, de Simon Singh (2001).

Durante anos, a necessidade de uma comunicação eficiente entre reis, rainhas e generais motivou a criação de mecanismos capazes de assegurar que informações sigilosas não fossem interceptadas. Um desses mecanismos de comunicação secreta é a Esteganografia que consiste em esconder a mensagem. Porém, esse mecanismo oferece pouca segurança, contribuindo assim para o desenvolvimento da Criptografia.

Um aparelho utilizado para criptografar mensagens é o Citale Espartano, composto por um bastão de madeira no qual é enrolada uma tira de couro contendo uma mensagem que desenrolada apresenta uma sequência aleatória de letras (Figura 1). A mensagem só será revelada quando enrolada em torno de um outro citale de mesmo diâmetro.

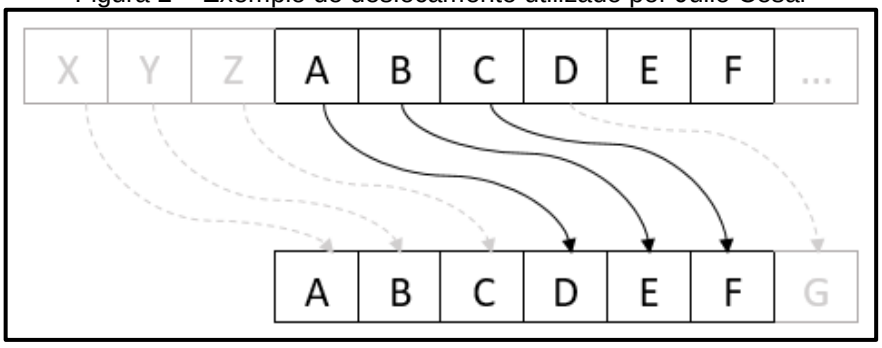
Figura 1 – Exemplo de Citale Espartano



Fonte: Singh (2001, p. 24).

Outro exemplo de Criptografia é a Cifra de César que consiste em deslocar o alfabeto em uma determinada quantidade de casas à frente (Figura 2). Essa especificação é conhecida como chave, que define o alfabeto cifrado exato que será usado na codificação.

Figura 2 – Exemplo de deslocamento utilizado por Júlio César

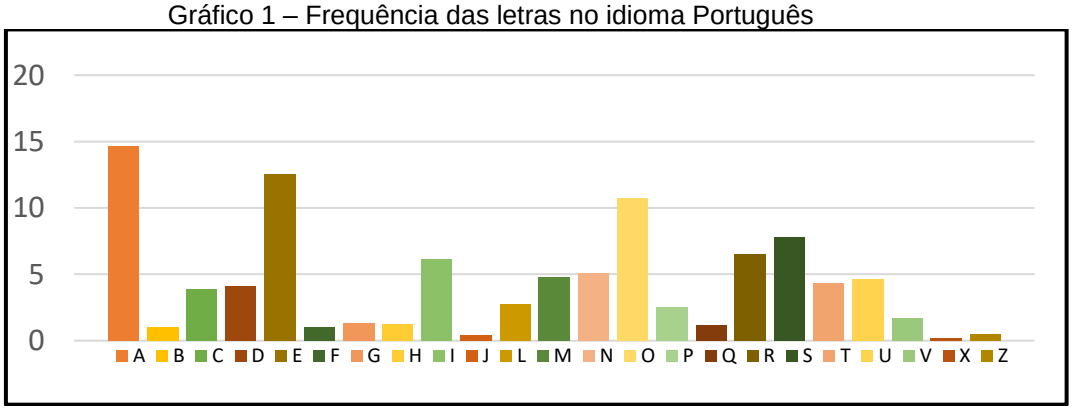


Fonte: Elaboração própria.

Muitos estudiosos achavam que esse tipo de cifra era inquebrável devido ao grande número de chaves envolvidas, contudo, surge a Criptoanálise, ciência que possibilita decifrar uma mensagem sem o conhecimento da chave.

A principal ferramenta da Criptoanálise é a análise de frequência. Essa técnica possibilita revelar o conteúdo de uma mensagem criptografada, analisando-se a frequência dos caracteres no texto cifrado de acordo com o idioma utilizado (Gráfico 1).

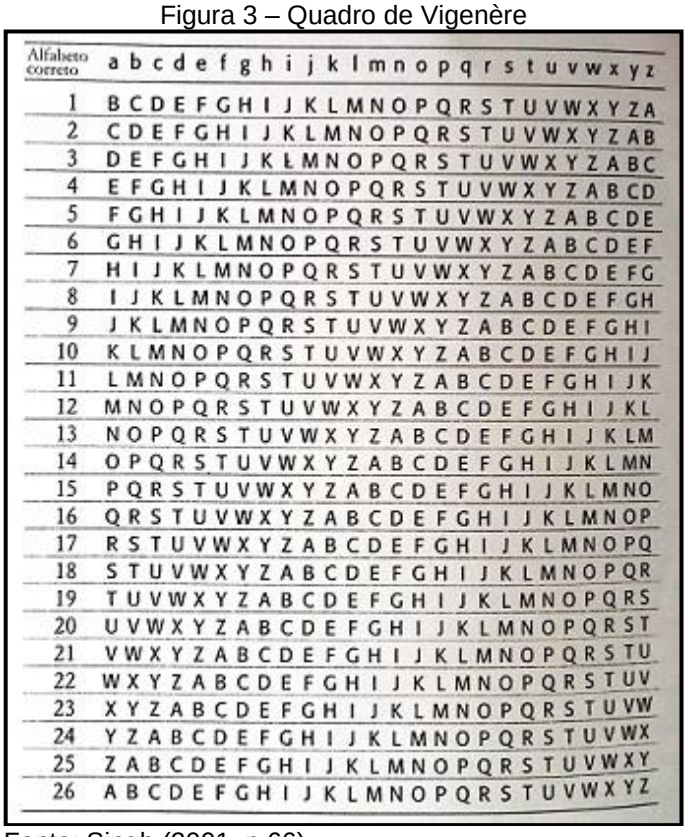
Gráfico 1 – Frequência das letras no idioma Português



Fonte: Elaboração própria.

Os processos que até então eram dados como seguros foram fragilizados, incitando a criação de cifras mais fortes, como a cifra de Vigenère, que consiste em uma tabela formada por 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior (Figura 3).

Figura 3 – Quadro de Vigenère

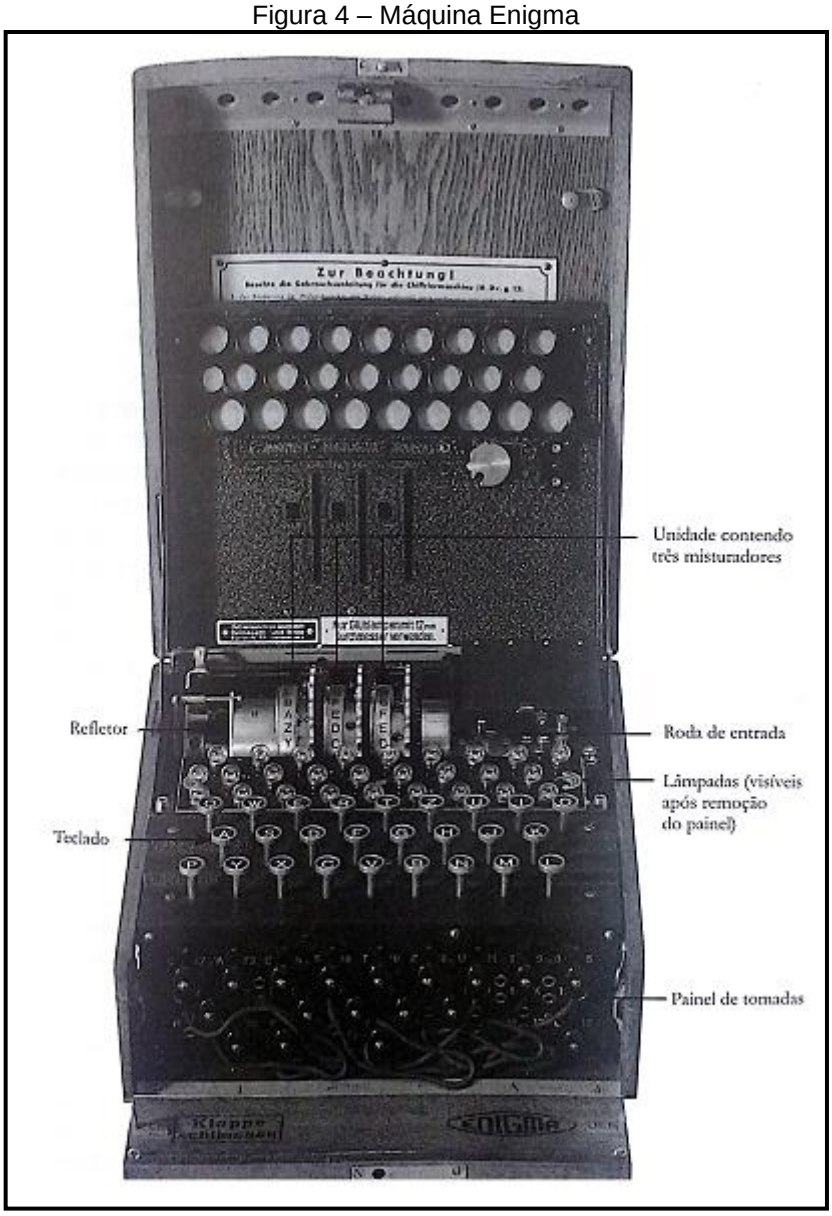


Alfabeto correto	a b c d e f g h i j k l m n o p q r s t u v w x y z
1	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
2	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
3	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
4	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
5	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
6	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
7	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
8	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
9	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
10	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
11	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
12	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
13	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
14	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
15	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
16	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
17	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
18	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
19	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
20	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
21	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
22	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
23	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
24	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
25	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
26	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Fonte: Singh (2001, p.66).

Durante a Segunda Guerra Mundial, os alemães utilizaram a máquina Enigma (Figura 4), para enviar mensagens criptografadas aos seus exércitos.

Figura 4 – Máquina Enigma



Fonte: Singh (2001, p. 159).

A Inglaterra convocou especialistas para decifrarem a Enigma. Dentre eles, destaca-se Alan Turing, que criou as bombas de Turing e quebrou a cifra da Enigma.

> Além das bombas de Turing, usadas para quebrar a cifra Enigma, os britânicos inventaram outro aparelho decifrador, o Colossus, para combater uma forma ainda mais poderosa de cifra, a cifra alemã Lorenz. Dos dois tipos de máquinas decifradoras, foi a Colossus que determinou o desenvolvimento da criptografia na segunda metade do século XX (SINGH, 2001, p.267).

Ao longo de sua história, a Criptografia foi prejudicada pela dificuldade na distribuição de chaves, pois antes da troca de mensagens era necessário o

compartilhamento da chave a ser utilizada, o que muitas vezes era realizado por uma terceira parte, e isto enfraquecia a segurança.

Com intuito de solucionar este problema, o criptógrafo Whitfield Diffie e o professor Martin Hellman começaram a realizar estudos de modo a encontrar uma alternativa de transportar fisicamente as chaves ao longo de grandes distâncias em segurança. Mais tarde, Ralph Merkle se uniu a eles nessa pesquisa.

Eles criaram um modelo de caixa com dois cadeados que não funciona na vida real, mas contribuiu na busca da solução do problema da distribuição de chaves. Eles voltaram suas pesquisas para as funções matemáticas, que são operações que transformam um número em outro. Mais especificamente, eles buscavam funções fáceis de fazer e difíceis de desfazer, chamadas de funções de mão única com o intuito de solucionar este problema, mas foram outros três pesquisadores que conseguiram criar a cifra mais influente da Criptografia moderna, a cifra RSA.

A Criptografia de chave pública RSA acabou com o problema da distribuição de chaves dando uma clara vantagem aos criptógrafos.

Com isso, cientistas tentam construir um novo computador capaz de realizar cálculos em velocidade avançada, os computadores quânticos, contribuindo para a quebra da RSA.

Experiências anteriores mostraram que cifras consideradas inquebráveis sucumbiram ao ataque de criptoanalistas. Prevendo a chegada dos computadores quânticos, os criptógrafos trabalham em uma solução que coloque um fim na batalha entre criadores e quebradores de códigos. Com base na teoria quântica, busca-se um sistema de cifragem inquebrável, a criptografia quântica.

2. PROPOSTA PEDAGÓGICA

A presente proposta pedagógica tem como objetivo apresentar os aspectos relevantes da história da Criptografia por meio de vídeos, slides explicativos, apresentação oral e atividades. Além disso, pretende-se mostrar a relação da Criptografia com o conteúdo matemático Função Afim e sua inversa. As atividades propostas serão estruturadas sob a forma de gincana, em que as realizadas individualmente contarão 1 ponto para cada resposta correta e as realizadas em grupo, 10 pontos cada. Cada aluno ou grupo que terminar primeiro a atividade proposta, receberá uma chave que servirá como bônus para a atividade final da gincana.

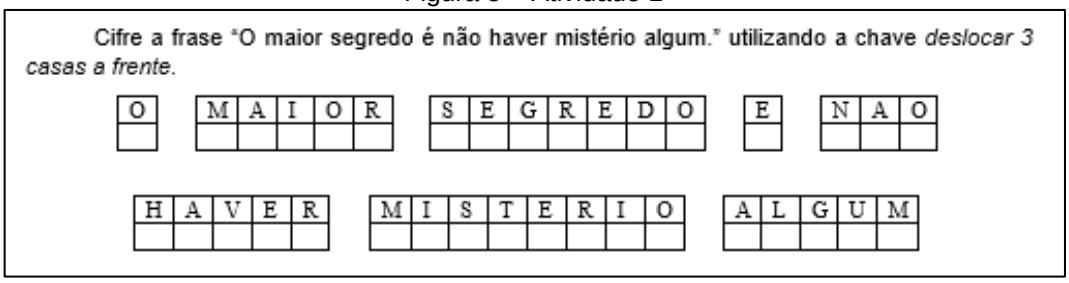
O minicurso iniciará com um questionamento aos participantes sobre o que já ouviram falar sobre Criptografia.

Será apresentado um vídeo (vídeo 1 – 00:00:25) contendo a definição de Criptografia, complementado pela explicação dos primeiros registros de utilização de mecanismos capazes de assegurar o sigilo na comunicação.

Dentre esses mecanismos, podemos citar alguns que serão apresentados aos participantes: Esteganografia (em slide e em exemplo concreto), Citale Espartano (em slide e em exemplo concreto), Cifra de César (em slide, material concreto e atividade 1).

Atividade 1 (individual): Esta atividade tem como objetivo fixar o processo utilizado por César para cifragem de mensagens (Figura 5).

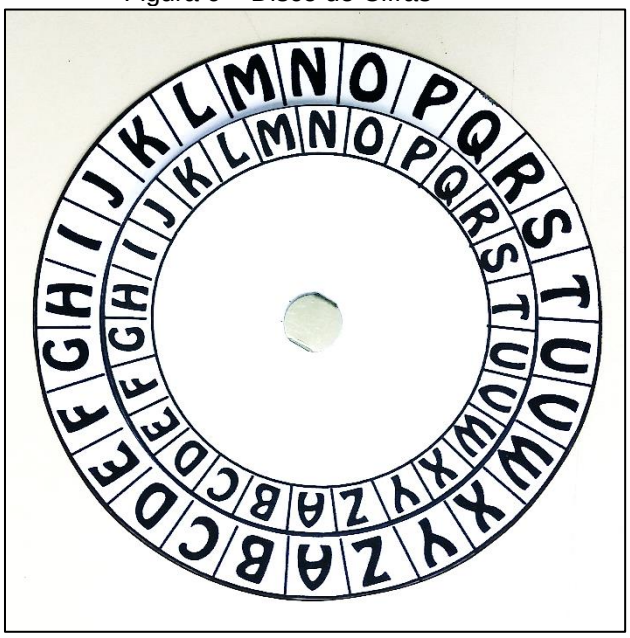
Figura 5 – Atividade 1



Fonte: Elaboração própria.

Para a realização desta atividade, cada participante receberá um disco de cifras (Figura 6) que o auxiliará nesse processo.

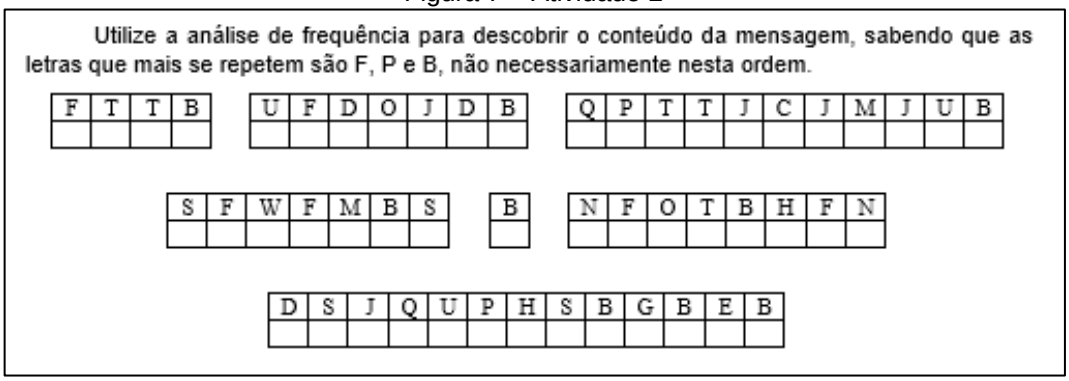
Figura 6 – Disco de Cifras



Fonte: Elaboração própria.

Em seguida, pretende-se apresentar definições de alguns termos que comumente são utilizados em Criptografia, tais como: cifra, cifra de transposição, cifra de substituição e código. Logo após, será feita uma breve explicação de que além de existirem métodos para cifragem de mensagens, existem também métodos que são utilizados para fazer o processo inverso, isto é, decifrar mensagens. Um desses métodos, conhecido como Análise de Frequência será apresentado em slides e com um pequeno vídeo (vídeo 2 – 00:01:36). Após a apresentação, os participantes realizarão a segunda atividade (Figura 7) cujo objetivo é decifrar uma mensagem utilizando o método Análise de Frequência.

Figura 7 – Atividade 2

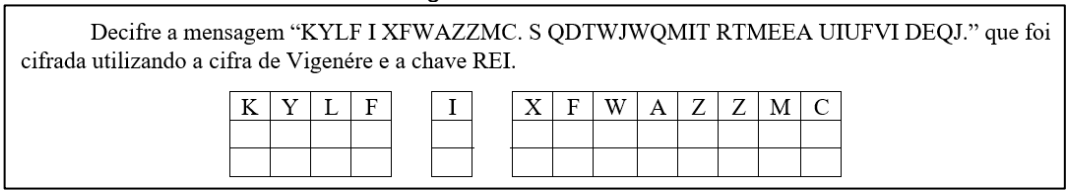


Fonte: Elaboração própria.

Uma breve discussão será levantada sobre a disputa que existe entre Criptógrafos (aqueles que constroem cifras) e os Criptoanalistas (os que criam métodos para decifrar mensagens). Será feita uma analogia entre o processo que existe entre bactérias e produção de antibióticos com a Criptografia.

Devido a crescente quebra de cifras por parte dos criptoanalistas, cifras mais fortes são criadas a todo momento. Um exemplo é a Cifra de Vigenère. Após explicação deste método (por meio de slides), os participantes realizarão a terceira atividade (Figura 8).

Figura 8 – Atividade 3



Fonte: Elaboração própria.

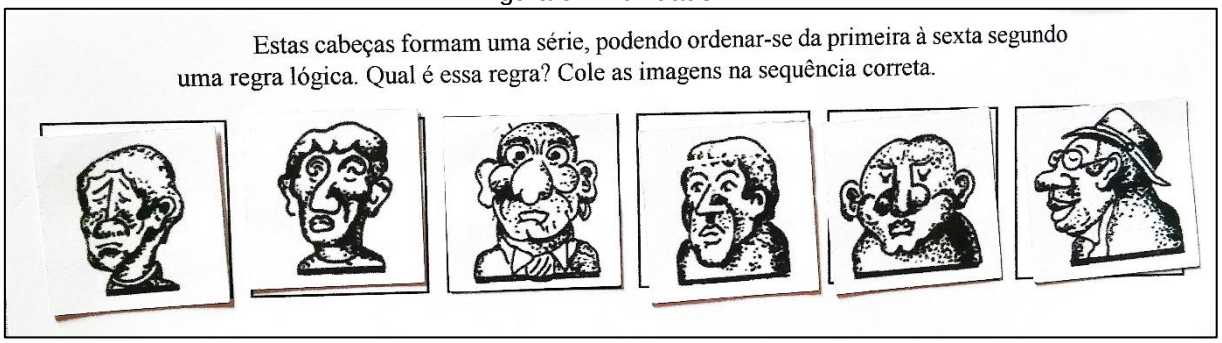
Terminada a atividade, serão apresentados alguns tópicos que retratam a evolução da Criptografia até os dias atuais: Máquina Enigma na Segunda Guerra Mundial (vídeo 3 – 00:00:31 e vídeo 4 – 00:05:55), popularização do computador,

problema da distribuição da chave, Troca de cadeados (vídeo 5 – 00:00:33), chave simétrica e chave assimétrica (vídeo 6 – 00:01:04), Cifra RSA, criptografia na atualidade, comentários sobre casos atuais e assuntos como: redes sociais, transações bancárias, urnas eletrônicas, etc.

Em seguida, os participantes serão divididos em grupos para realização das outras atividades.

Atividade 4 (Esteganografia): Nesta atividade, cada grupo receberá uma sequência aleatória de faces contendo números, aparentemente escondidos, e deverão encontrar a sequência correta colando em seguida em uma ficha recebida (Figura 9).

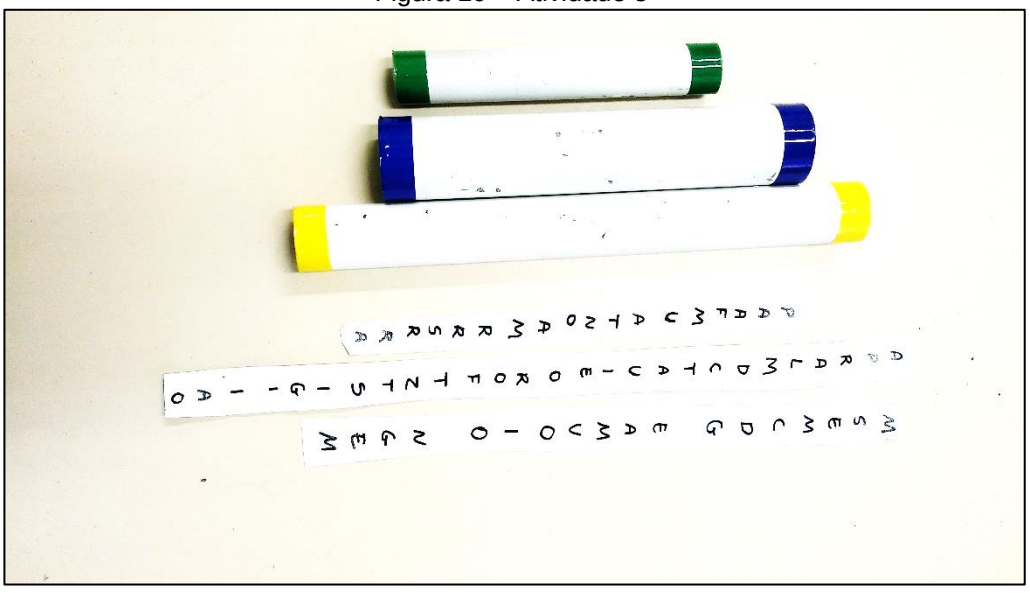
Figura 9 – Atividade 4



Fonte: Elaboração própria.

Atividade 5 (Citale Espartano): Cada grupo receberá três bastões de PVC com diferentes diâmetros e três tiras com letras aleatórias (Figura 10), com o objetivo de descobrir uma mensagem oculta enrolando cada tira de papel no bastão correspondente.

Figura 10 – Atividade 5



Fonte: Elaboração própria.

Atividade 6: Cada grupo receberá uma ficha contendo a questão abaixo (Figura 11) em que deverão, ao seguir os passos propostos, identificar o mecanismo de cifragem utilizada e decifrar a mensagem.

Figura 11 – Atividade 6

(Fatec – 2017): Maria, aluna da Fatec Mococa, para garantir a segurança das mensagens que pretende transmitir, criou um sistema de criptografia da seguinte forma:

- montou uma tabela de 2 linhas e 13 colunas para colocar as 26 letras do alfabeto, sem repetição de letra;
- nas cinco células iniciais da 1ª linha, da esquerda para a direita, escreveu, uma a uma, as letras F, A, T, E, C nessa ordem;
- ainda na 1ª linha, na 6ª célula, da esquerda para a direita, obedecendo a ordem alfabética (de A a Z) colocou a primeira letra ainda não utilizada nas células anteriores;
- da 7ª célula a 13ª célula da 1ª linha, inseriu sete letras, da esquerda para a direita, sem repetir letra, seguindo a ordem alfabética, começando pela primeira letra ainda não utilizada nas células anteriores;
- preencheu a 2ª linha, da esquerda para a direita, com as letras restantes do alfabeto, também em ordem alfabética e sem repetição de qualquer letra já utilizada anteriormente.

A tabela mostra o início do processo, com as seis primeiras letras.

F	A	T	E	C	B							

Tendo construído a tabela conforme o descrito, para criptografar uma mensagem, Maria substitui cada letra da 1ª linha pela que está na 2ª linha, na mesma coluna, e vice-versa. A acentuação, a pontuação e o espaço entre as palavras são desconsiderados.

Assim, para desejar BOA PROVA para uma colega, que sabia fazer a decodificação, escreveu RTNEBTHN.

Para João, que também sabia decodificar a mensagem, Maria escreveu:

AGAQNENBPSPNEBPASPB

A partir da decodificação, João entendeu que a mensagem de Maria foi:

a) Nunca pare de aprender
b) Nunca deixe de estudar
c) Nunca faça isso de novo
d) Sempre tire boas notas
e) Sempre faça boas ações

Fonte: Elaboração própria.

Finalizada a atividade, cada grupo receberá um disco de cifra contendo letras (círculo menor) e números (círculo maior), para utilizar na próxima atividade. O objetivo desta etapa é apresentar aos participantes a relação entre a função afim e sua inversa com a Criptografia.

Atividade 7: Nesta atividade (Figura 12), os grupos deverão cifrar numericamente a mensagem utilizando o disco e determinar a função afim que representa a chave utilizada no processo.

Figura 12 – Atividade 7

Utilizando a palavra CODIGO:

a) Indique a sequência numérica associada;

C	O	D	I	G	O

b) Cifre usando a chave "avance quatro casas", e indique a nova sequência numérica;

c) Escreva a mensagem cifrada.

d) Como a chave cifradora poderia ser escrita em linguagem matemática?

Fonte: Elaboração própria.

Atividade 8: Cada grupo deverá cifrar uma mensagem utilizando a função afim dada como chave (Figura 13).

Figura 13 – Atividade 8

Cifre a palavra C R I P T O G R A F I A, utilizando a função cifradora $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = 3x + 1$.

Fonte: Elaboração própria.

Atividade 9: Nesta atividade, cada grupo deverá descobrir a mensagem cifrada, utilizando a função inversa da função afim dada (Figura 14).

Figura 14 – Atividade 9

A mensagem T M A C A M L Q C E S G S foi cifrada a partir da função cifradora $f: \mathbb{Z} \to \mathbb{Z}$ definida por $f(x) = x - 2$. Você seria capaz de descobrir a mensagem original?

Fonte: Elaboração própria.

Atividade 10: Nesta atividade (Figura 15) será necessário cifrar e decifrar mensagens (itens a e b) e, em seguida, resolver os demais itens utilizando o raciocínio lógico, além dos demais mecanismos apresentados.

Figura 15 – Atividade 10

(OBMEP, 2007 – Adaptada) Utilizando a chave “avance quatro casas”, a palavra PAI é cifrada como 20 – 5 – 13.

a) Cifre OBMEP usando a chave “avance dezenove casas”.
b) Usando a chave “avance 7 casas”, descubra qual palavra foi cifrada como 14 – 12 – 22 – 20 – 12 – 27 – 25 – 16 – 8.
c) Bernardo cifrou uma palavra de 4 letras com a chave “avance dezenove casas”, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Bernardo colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele cifrou.
d) Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?

Fonte: Elaboração própria.

Para finalizar a gincana, será proposta como última atividade a abertura de um cadeado (Teste de força bruta). Para tanto, cada grupo deverá utilizar suas chaves conquistadas para tentativas de abertura. O grupo que conseguir abrir o cadeado, ganhará 10 pontos.

3. CONSIDERAÇÕES

Espera-se com essa proposta de minicurso, difundir a Criptografia que é um tema abrangente e atual, e sua história que é bem rica e interessante, possibilitando aos alunos, futuros professores e professores um estudo acerca deste tema relacionado ao conteúdo de função afim e sua inversa, proporcionando significado à aprendizagem.

REFERÊNCIAS

BORGES, Fábio. Criptografia como Ferramenta para o Ensino de Matemática. In: Congresso Nacional de Matemática Aplicada e Computacional (CNMAC), 31., 2008, Belém. **Anais...** Belém: Sociedade Brasileira de Matemática Aplicada e Computacional, 2008. p. 822-828. Disponível em: <http://www.sbmac.org.br/eventos/cnmac/xxxi_cnmac/PDF/189.pdf>. Acesso em: 26 dez. 2016.

BRASIL. Secretaria da Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais para o Ensino Médio.** Brasília: MEC, 2002.

PEREIRA, Nádia Marques Ikeda. **Criptografia**: uma nova proposta de ensino de matemática no ciclo básico. 2015. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista Júlio de Mesquita Filho, Ilha Solteira, 2015. Disponível em: < http://repositorio.unesp.br/bitstream/handle/11449/127733/000844677.pdf?sequence=1&isAllowed=y>. Acesso em: 26 dez. 2016.

PEREIRA, Viviane da Silva Stellet. **Ensino de Funções:** Uma Abordagem Contextualizada Sobre o Tratamento da Informação no Ensino Médio. 2012. Dissertação (Mestrado em Educação Matemática) – Universidade Severino Sombra, Vassouras, 2012.

SANTOS, José Luiz dos. **A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica.** 2013. Dissertação (Mestrado Profissional em Matemática em Rede Nacional – PROFMAT) – Instituto de Matemática, Universidade Federal da Bahia, Salvador, 2013. Disponível em: < http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/208/2011_00046_JOSE_LUIZ_DOS_SANTOS.pdf?sequence=1>. Acesso em: 26 dez. 2016.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. Tradução de Jorge Calife. Rio de Janeiro: Record, 2001.

TAMAROZZI, Antonio Carlos. Codificando e decifrando mensagens. **Revista do Professor de Matemática**, São Paulo: Sociedade Brasileira de Matemática, n. 45, p. 41-43, 2001.