O ENIGMA: EXPLORANDO AS POSSIBILIDADES DIDÁTICAS DA CRIPTOGRAFIA ATRAVÉS DE UM JOGO

Diego Sales da Costa[1]

História da Matemática, História da Educação Matemática e Cultura

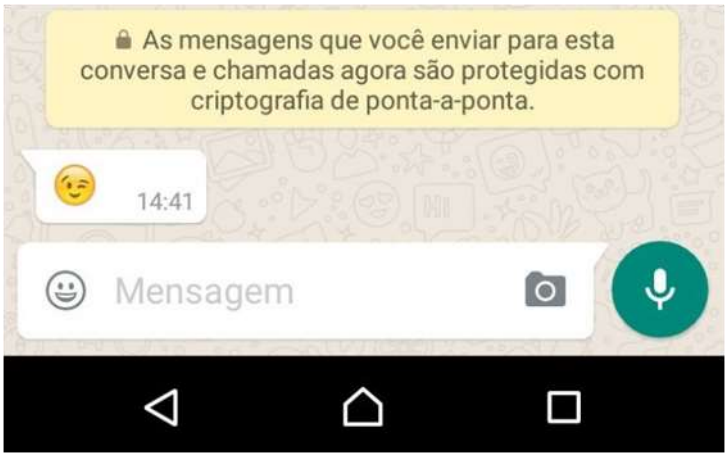
Resumo: A presente oficina tem por objetivo introduzir o conceito de criptografia, a partir de uma abordagem histórica desde os tempos dos Romanos até a sua utilização na informática através do matemático inglês Alan Turing (1912-1954) que contribuiu com a vitória dos aliados na segunda guerra mundial, desvendando suas mensagens secretas produzidas pela máquina *Enigma.* O trabalho justifica-se devido às inúmeras aplicações da criptografia em nosso cotidiano, podendo ser encontrada no envio de mensagens de rede sociais e também em códigos de segurança bancários. Desta forma o professor pode aplicar de diferentes modos em sala de aula utilizando para exercício, introdução e revisão de assuntos como regra de três, equações e matrizes, de uma maneira instigante e motivacional, através de situações cotidianas e aplicações que fazem parte da vida do aluno.
Palavras Chaves: Criptografia. História da criptografia. Educação Matemática. Alan Turing. Enigma.

1 INTRODUÇÃO

A palavra criptografia é oriunda do grego, *cryptos,* que significa oculto. A criptografia estuda os modos de se codificar uma mensagem de modo que apenas o seu destinatário consiga decifrá-la.

Na atualidade é comum encontrar a palavra criptografia, principalmente relacionado à segurança bancária ou até mesmo em redes sociais, como podemos ver na figura 1, a seguir.

Figura 1 - Mensagem do whatsapp



Fonte: www.ebc.com.br[2]

[1] Licenciando em Matemática. Universidade Federal do Rio Grande do Norte. E-mail:diego.sales33@gmail.com

[2] Disponível em: <http://www.ebc.com.br/sites/_portalebc2014/files/styles/full_colunm/public/atoms_image/mensagem_criptografia_whatsapp.jpg?itok=jGEpJdBn>

A figura 1 apresenta um *print* da rede social *whatsapp* que apresenta uma mensagem relacionada à criptografia. Um dos métodos mais conhecidos de criptografia é o RSA, um método de chave pública. Inventado em 1977, o código basicamente se vale de uma multiplicação entre números primos compostos por vários algarismos, ou seja, extremamente grandes.

A proposta deste trabalho é utilizar-se da criptografia para revisar conteúdos matemáticos de maneira instigante ou como introdução a assuntos da teoria dos números, como por exemplo: números inteiros, números primos, divisores e múltiplos. Isto será feito utilizando-se de um jogo, onde os alunos devem decifrar códigos utilizando os seus conhecimentos matemáticos e avançando de fase até alcançar o objetivo, onde receberão uma recompensa. Esta atividade será feita após imersão em um contexto histórico onde a criptografia foi essencial, a segunda guerra mundial.

2 CRIPTOGRAFIA E A HISTÓRIA

2.1 A cifra de César

O general Júlio César (100-44 a.C) foi um ditador romano a quem é atribuída a criação de um código para comunicar-se com as legiões romanas em combate. Este código consistia na substituição das letras seguindo uma ordem determinada. Um maneira de decifrar este tipo de código é através do dispositivo prático da figura 2, a seguir.

Figura 2 - Exemplo de dispositivo para decifrar a Cifra de César

Fonte: www.clubedosgeeks.com.br[3]

De acordo com a Figura 2, considerando que o arco de raio maior seja o código que queremos escrever, com a chave 25 a palavra CASA, por exemplo, seria escrita como BZRZ. [3]

Segundo Coutinho (2015) o problema deste tipo de código é a facilidade com ele pode ser decifrado mesmo sem saber qual é a sua chave. Isto acontece, pois a frequência de repetição de uma determinada letra em um idioma é mais ou menos constante. Por exemplo, na língua portuguesa as letras que mais se repetem é são A, E e O. Para constatar isto, basta observar uma página de um texto qualquer.

2.2 A segunda guerra mundial e as contribuições de Alan Turing

A guerra mundial foi um conflito bélico ocorrido entre 1939 e 1945. As principais potências envolvidas foram Itália, Alemanha e Japão compondo o Eixo e Estados Unidos, Grã-Bretanha e França, denominados de Aliados. Para enviar mensagens de guerra, a Alemanha nazista utilizava uma máquina eletromecânica denominada *enigma,* seus códigos eram considerados indecifráveis devido a constante mudança das chaves utilizadas para decifrar os códigos. Entretanto, uma equipada comandada pelo matemático Alan Turing conseguiu solucionar os códigos da máquina enigma.

[3] Disponível em: <http://clubedosgeeks.com.br/wp-content/uploads/2014/05/logo.jpg>

Alan Turing (1912-1945) foi um matemático britânico que durante a segunda guerra mundial coordenou a equipe capaz de decifrar o código enigma, um dos dispositivos teóricos desenvolvidos por ele foi denominado com seu nome, a máquina de Turing. Em 1952, Turing sofreu processo judicial por ser homossexual. Submetido à castração química, suicidou-se em 1954, ingerindo cianeto. Parte da vida de Alan Turing foi retratada no drama O jogo da imitação (2015).

3 ROTEIRO DE ATIVIDADES

Para construção desta atividade foram necessários, envelopes, folhas A4, folhas de caderno, canetas, cadeado de números, caixa e recompensa.

Passo 1: Inserir os participantes na atmosfera do jogo.

Breve explanação sobre o que é a criptografia, sobre a segunda guerra mundial e a vida de Alan Turing. Se possível mostrar o trailer do filme ou o filme completo.

Passo 2: Ensinar o que é a Cifra de César e construir um dispositivo para decifrá-la

Material: Caneta, folhas de caderno e tesoura.

Escreva o alfabeto duas vezes em uma folha de caderno.

Recorte em forma de tiras.

Vamos testar o dispositivo?

Passo 3: Ensinar como utilizar a Cifra de César

Para decifrar um código, basta deixar uma das tiras fixas, esta tira será referente ao código que deseja-se decifrar. A segunda tira será deslocar a quantidade de vezes dada pela chave, os resultados obtidos devem ser anotados.

Exemplos de códigos para serem decifrados:

Mensagem: PDWHPDWLFD

Chave = 3

Qual a resposta?

MATEMATICA

Mensagem: MBSZDYQBKPSK

Chave = 10

Qual a resposta?
CRIPTOGRAFIA

Mensagem: ZSNAZWXNIFIJ QZYJWFSF
Chave = 5
Qual a resposta?
UNIVERSIDADE LUTERANA

Mensagem: DBOPBT SJP HSBME EP TVM
Chave = 1
Qual a resposta?
CANOAS RIO GRANDE DO SUL

Passo 4: Explicação do jogo *O enigma*

Estas são as regras do jogo uma das possibilidades do jogo está no Apêndice. Nesta opção foram utilizados conhecimentos prévios de regra de três composta, equação do segundo grau e determinantes.

1. Você e seus amigos agora fazem parte da equipe de Alan Turing. O objetivo do jogo é decifrar os códigos e avançar mais rápido que os inimigos.

2. O jogo é composto de 2 etapas:

Em cada etapa o grupo recebe um envelope com uma mensagem recebida do posto de observação e uma mensagem para ser decifrada. A mensagem do posto de observação é uma dica que contém o segredo para decifrar a mensagem. A mensagem está escrita na Cifra de César. As mensagens serão utilizadas para vencer o jogo. Por isso, devem estar completas. Vence o grupo que conseguir abrir o cadeado primeiro. Ao obter o código para decifrar o Enigma o grupo deve levantar a mão e chamar o fiscal.

3. Ao terminar de decifrar uma mensagem outra deve ser pedida ao fiscal.

4. Não é permitido o uso de dispositivos eletrônicos.

5. Dica: Trabalhem em grupo dividindo as tarefas e utilizem os conhecimentos dados no início da oficina.

Boa sorte!

4 POSSIBILIDADES DE ADAPTAÇÃO

As condições de realização desta atividade podem variar. Caso o professor não tenha os instrumentos necessários para transmitir o filme ou o trailer, pode-se pedir para que os alunos o façam em casa. A atividade pode ser feita de maneira interdisciplinar com outras disciplinas como, por exemplo, a disciplina de História. Neste caso, o professor de História pode abordar o contexto histórico da segunda guerra mundial, enquanto o professor de Matemática utiliza este contexto histórico para inserir os assuntos matemáticos que deseja abordar.

A oficina pode ser utilizada para os alunos despertarem o interesse pela aritmética básica, se aplicada antes de lecionar assuntos como fatoração, múltiplos e divisores, números primos. Geralmente estes assuntos são explorados no ensino fundamental. O professor pode ainda utilizar das mensagens do posto de observação presentes no jogo para inserir qualquer problema sobre qualquer assunto, basta que o problema forneça uma resposta numérica que será a chave do código. Por exemplo, o professor pode inserir problemas sobre funções polinomiais do segundo grau, questões para achar as raízes, o eixo de simetria ou o sentido da concavidade da parábola.

Neste caso, é importante ressaltar que quanto mais complexos os problemas ou quanto maiores as mensagens mais tempo os alunos levarão para decifrar os códigos. O professor pode alterar o tempo necessário para realização da atividade também com a quantidade de mensagens a serem decifradas. É de vital importância para o funcionamento do jogo que as mensagens e os problemas sejam rigorosamente verificados.

Quanto ao material utilizado o professor pode personalizar o material, por exemplo, inserir carimbos nos envelopes e escrever com caneta o nome confidencial ou *não abrir.* Isto ajuda os alunos a se inserirem no clima do jogo. Além disso, o cadeado pode ser trocado por outro dispositivo basta que o professor use a criatividade. A recompensa também pode ser simples como um saco de pirulitos, mas é importante que haja alguma, pois o jogo gera uma expectativa nos participantes.

No mais, fica a critério do professor as adaptações necessárias para implementação desta oficina em sala de aula. De todo modo, os temas podem ser abordados de maneira lúdica, explorando uma sadia competição.

5 REFLEXÕES FINAIS

O objetivo desta oficina é utilizar a criptografia de uma forma didática, fazendo uma abordagem interdisciplinar através de um viés histórico. Desse modo, acredita-se que os alunos sintam-se mais motivados na aprendizagem dos conteúdos. Os recursos manipulativos podem ser grandes aliados do professor no ensino da Matemática. Além disso, esta é uma forma simples de apresentar ao aluno um pouco da matemática que está presente nas diversas tecnologias existentes atualmente.

Assim, espera-se que os professores consigam aplicar esta oficina de maneira satisfatória, tornando o processo de ensino aprendizagem mais dinâmico e divertido.

5 REFERÊNCIAS

COUTINHO, S. C. Criptografia. Rio de Janeiro: IMPA, 2015. 217 p.

DE JESUS, André Luis Neres. Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes. 2010. Disponível em: <http://bit.profmat-sbm.org.br/xmlui/handle/123456789/872>. Acesso em: 22 de Maio. 2017.

FIARRESGA, Victor Manuel Calhabrês. Criptografia e Matemática. 2010. Disponível em:<https://repositorio.ul.pt/handle/10451/3647> . Acesso em 21 de Maio de 2017.

GROENWALD, C. L. O.; OLGIN, C. A. Criptografia e Conteúdos de Matemática do ensino Médio. In: CNEM – Congresso Nacional de Educação Matemática, 2011, Ijuí. Revista CNEM, 2011.

O JOGO da Imitação. Direção: Morten Tyldum, Produção: Black Bear Pictures; Bristol Automotive, 2015.

6 APÊNDICE

Jogo

Mensagem do posto de observação 1:

As raízes das equações fornecem coordenadas de lançamentos de projeteis inimigos:

$x^2 + 5x – 6 = 0$

$x^2 – 7x + 10 = 0$

$x^2 + 3x = 0$

$x^2 – 5\,x – 6 = 0$

$x^2 – 16x + 60 = 0$

A soma das raízes de todas as equações é a chave para decifrar a mensagem 1.

Mensagem 1: UAILU PIWY ZUT JULNY XU YKOCJY XY UFUH NOLCHA.

Mensagem do posto de observação 2:

Os alemães estão descarregando caminhões para construir um forte, sabe-se que em 8 horas, 20 caminhões descarregam $160m^3$ de areia. Em 5 horas, quantos caminhões serão necessários para descarregar $125m^3$?

A soma dos algarismos do resultado do problema nos da a chave para decifrar a mensagem 2.

Mensagem 2:

VZ HSPHKVZ LZAHV WYLWHYHUKV BT NYHUKL KLZLTIHYXBL UH UVYTHUKPH.

Mensagem do posto de observação 3:

As raízes das equações fornecem coordenadas de lançamentos de projeteis inimigos:

$x^2 + x – 12 = 0$

$x^2 – 2x - 8 = 0$

$4x^2 - 20x + 9 = 0$

$x^2 - 4 = 0$

$x^2 + 5x + 6 = 0$

A soma das raízes das de todas as equações é a chave para decifrar a mensagem 3:

Mensagem 3:

P HFOFSBM FJTFOIPXFS QBSBCFOJAB TVB FRVJQF QFMP FNQFOIP FN EFDJGSBS BT NFOTBHFOT EP JOJNJHP

Mensagem 4:

DV FLGDGHV DOHPDHV HVWDR XPD D XPD FDLQGR VREUH R GRPLQLR DOLDGR IDOWD DSHQDV XPD HWDSD SDUD TXH D JXHUUD VHMD ILQDOPHQWH HQFHUUDGD

Mensagem do posto de observação 4:

O determinante da matriz A fornece a quantidade de tanques inimigos em uma cidade:

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

A chave para decifrar a mensagem 4 é o resultado do determinante:

Segunda fase

O código do cadeado para solucionar *O ENIGMA* é composto por três números.

A quantidade de letras A na primeira mensagem mais a quantidade de letras G nas duas primeiras mensagens menos a quantidade de letras A na segunda mensagem é o primeiro digito da senha.

O segundo digito é quantidade de letras W contidas nas 4 mensagens.

O terceiro digito é quantidade de letras K nas 4 mensagens.