O ENSINO LÚDICO DE MATRIZES COM A CRIPTOGRAFIA

Ana Carolina Nepomuceno Costa [1]

RESUMO

Este trabalho trata das experiências vividas por bolsistas do Programa Institucional de Bolsa de Iniciação à Docência (PIBID) / IFCE campus Fortaleza, no Colégio Estadual Presidente Humberto Castelo Branco, em turmas do 2º ano do Ensino Médio. Com o propósito de chamar a atenção dos alunos, foi aplicado o jogo "Qual a senha?", com o objetivo de avaliar o aprendizado sobre multiplicação de matrizes usando a criptografia da matriz para criptoanálise. As aulas foram ministradas utilizando-se de estratégias que estimula e chama atenção dos alunos, baseado na metodologia interativa em que assuntos de interesse dos alunos fizessem parte do conteúdo que estava sendo lecionado, que foi o uso de matrizes e a relação com a criptografia.

Palavras-chave: Ensino de Matemática, Criptografia, IFCE, PIBID, Criptoanálise.

INTRODUÇÃO

Este trabalho trata das experiências vividas por bolsistas do Programa Institucional de Bolsa de Iniciação à Docência (PIBID)/IFCE *campus* Fortaleza no Colégio Estadual Presidente Humberto Castelo Branco entre os meses de março e maio de 2016. As aulas foram ministradas utilizando-se de estratégias que estimulam e chamassem a atenção dos alunos, baseado na metodologia interativa em que assuntos de interesse dos alunos fizessem parte do conteúdo que estava sendo lecionado.

A princípio foi-se repassado aos alunos a real utilização das matrizes e o quão eram importantes, principalmente nas Guerras, e assim eles mostraram-se instigados e mais interessados no conteúdo. Ademais com a interdisciplinaridade, eles puderam ver que há relação da disciplina de matemática com as outras matérias.

Após os esclarecimentos do uso da criptografia e todo o seu contexto, foi introduzido um jogo criado pelos bolsistas chamado "qual a senha? " em que há a matriz identidade que, multiplicada com as outras, dá um resultado e, a partir disso, cada número é um caractere, por exemplo, o número "1" seria a letra "A" e assim por diante. O resultado da multiplicação das matrizes dá uma dica de um filme a ser descoberto.

[1] Graduada do Curso de Licenciatura em Matemática do Instituto Federal de Ciência Educação e Tecnologia do Ceará - IFCE, carolina.nep@gmail.com;

METODOLOGIA

Foi feita uma pesquisa de campo no Colégio Estadual Presidente Humberto Castelo Branco, em várias turmas do 2º ano do Ensino Médio, onde aplicamos o jogo “Qual a senha?” com o objetivo de avaliar os resultados positivos usando a criptografia da matriz para criptoanálise. Diante disso, foi utilizado um método bastante simples que envolve matrizes inversas.

A pesquisa foi desenvolvida com base no teórico Al-Kadit (1992), onde este relata sobre a história da matemática em geral, principalmente a descoberta na Arábia. Segundo ele:

> Manuscritos antigos recentemente descobertos mostram que a origem da criptologia e as contribuições árabes para ela são mais antigas e mais extensas do que se pensava anteriormente. A palavra "cifra" nas línguas européias vem da palavra árabe *sifr* . O cientista árabe do século IX al-Kindī é o autor do mais antigo livro conhecido sobre criptologia, anterior a qualquer outro por mais de 300 anos. (Al-Kadit, 1992)

Então toda a história da matemática e da criptografia no presente artigo é com base nesse autor. Além disso, utilizamos dos conhecimentos de Barbosa (1972) e Borin (1998), que relata sobre o ensino de matemática na questão de resolução de problemas. Como bem relata os autores:

> [...]a resolução de problemas é a mais adequada para desenvolver uma postura crítica ante qualquer situação que exija resposta. Cada hipótese formulada ou cada jogada desencadeia uma série de questionamentos, como por exemplo, aquela seria a única jogada possível? Se houver outras alternativas, qual escolher e por que escolher entre esta ou aquela? Terminado o problema, quais os erros e por que foram cometidos? Ainda é possível resolver o problema ou vencer o jogo, se forem mudadas as regras? (Barbosa, 1972, p. 6, apud BORIN, 1998)

Percebendo isto, foi decidido aplicar este jogo com o intuito da resolução de problemas matemáticos e ainda contextualizado para que os alunos possam se interessar mais.

Colocamos, ainda, como importante ferramenta o protagonismo do aluno, destacando o seu crescimento para saber fazer em grupo e ajudar o outro, mas sempre com o professor como mediador do processo. De acordo com Barbosa e Borin:

> [...]para se alcançar um bom resultado com jogos é necessário que os alunos saibam trabalhar em grupo”: somente com o trabalho em grupo, haverá condições para se construir um ambiente onde haja reflexão a partir da observação e da análise cuidadosa, constituindo-se então essencial a troca de opiniões e a oportunidade de argumentar com o outro, de modo organizado. (Barbosa, 1972, p. 6, apud BORIN, 1998)

Outro ponto de vista a ser visto é como o aluno vê a disciplina de matemática que sempre é uma matéria de ensino verticalizado e, utilizando jogos e aulas diferentes modifica a ideia de que o ensino de matemática é sempre tradicional, expositiva, onde o professor é a figura central da sala de aula, como bem explicitado pelos autores:

> [...] essa metodologia representa, em sua essência, uma mudança de postura em relação ao que é ensinar matemática, ou seja, ao adotá-la, o professor será um espectador do processo de construção do saber pelo seu aluno, e só irá interferir ao final do mesmo, quando isso se fizer necessário através de questionamentos, por exemplo, que levem os alunos a mudanças de hipóteses, apresentando situações que forcem a reflexão ou para a socialização das descobertas dos grupos, mas nunca para dar a resposta certa. Ao aluno, de acordo com essa visão, caberá o papel daquele que busca e constrói o seu saber através da análise das situações que se apresentam no decorrer do processo. (Barbosa, 1972, p. 6, apud BORIN,1998, p. 10 – 11)

Assim, a mudança de postura do professor para planejar sua aula e trazer à sua classe uma ideia de aula de matemática divertida e inovadora é extremamente importante para o aprendizado do aluno, pois atualmente, com os avanços tecnológicos, a dispersão em sala está cada vez mais fácil, e o aluno, infelizmente, não absorvendo um certo conteúdo porque a aula é a mesma, acaba pendendo para o que ele considera mais “divertido”.

DESENVOLVIMENTO

A criptografia é o estudo de estratégias onde a informação pode ser modificada da sua forma inicial para outra indecifrável, tal que possa ser entendida somente por seu receptor. De acordo com Flávio Medeiros em “Uma breve história sobre criptografia”: “Criptografia, junção de duas palavras gregas κρυπτός (kriptós – secreto, escondido) e γράφειν (gráfein – escrita), é, resumindo, o uso de técnicas para transformar texto ou dados legíveis em informação ilegível, que não possa ser compreendida. ”

A criptografia surgiu há muito tempo e, desde o Egito Antigo foram feitas de vários tipos. A primeira, sendo encontrada o seu primeiro registro em hieróglifos no Antigo império do Egito, não foi considerada criptografia, mas sim mensagens misteriosas. Outras práticas encontradas foram na Mesopotâmia, utilizadas para proteger informações. Mais tarde os hebreus utilizaram a alteração do alfabeto. Estas foram chamadas de criptografia clássica (que é aquela usada por um mecanismo simples).

Logo após o período clássico veio a criptografia medieval, usada principalmente com o propósito religioso, como por exemplo, o Alcorão, em que foi criada a técnica de

substituição monoalfabética, em que cada letra é substituída por uma cifra, onde essa descoberta foi a mais relevante até o período da Segunda Guerra. Al-Kadit, um matemático árabe, iniciou os estudos sobre criptografia e criptoanálise (técnica de decifrar a mensagem criptografada), dentre outros estudiosos que pesquisaram sobre a cifra de substituição múltipla, cujo cada letra é trocada por um texto, e também a utilização de tabelas de análise frequência, onde se descobre os padrões de um determinado texto criptografado (AL-KADIT, 1992).

Depois, a criptografia ficou mais conhecida no período de guerras, como Guerra da Crimeia com Charles Babbage quando tenta encontrar fragilidades no sistema. Outro nome relevante para a história da criptografia foi Edgar Allan Poe em 1840, no qual procura desvendar códigos de cifras. Na Primeira Guerra o destaque foi a quebra da linguagem criptografada naval. A mais conhecida foi no período anterior à época da Segunda Guerra Mundial, desenvolvida com métodos matemáticos, utilizando estatística para criptoanálise.

O uso das máquinas de codificação teve papel importante, pois mesmo sendo manuais, era um avanço tecnológico, mesmo feito em segredo. Um renomado para a evolução da criptografia foi Claude Shannon, no qual trabalhou com a proteção da comunicação, sendo este o principal estudo para o início da era da criptografia moderna. Além do mais, a utilização da criptografia moderna tem só crescido após a Segunda Guerra Mundial, estudos matemáticos mais desenvolvidos em criptografia e criptoanálise foram possíveis graças à internet e ao avanço da tecnologia. Ademais, os estudos passaram a ser públicos com vários projetos para desenvolver informações seguras através de máquinas eletrônicas para empresas. Em seguida, outra descoberta foi a chave pública, em que a chave é um conjunto de códigos, que ao ser trocada nas comunicações através de um canal seguro, o sistema criptografa protegendo as informações. Um exemplo prático, no nosso dia a dia é a utilização do aplicativo Whattsapp, onde diz que as mensagens são protegidas com criptografia de ponta-a-ponta.

Tendo em vista o que foi mencionado, com o avanço da criptografia e criptoanálise as cifras, com o tempo, foram ficando com mais qualidade consideradas inquebráveis, porém a tecnologia computacional progride e fica mais acessível para a quebra.

A partir da história da criptografia abordada, foi feita uma pesquisa de campo no Colégio Estadual Presidente Humberto Castelo Branco, em duas turmas do 2º ano do Ensino Médio, onde aplicamos o jogo “Qual a senha?” com o objetivo de avaliar os resultados positivos usando a criptografia da matriz para criptoanálise.

Para o desenvolvimento do jogo foi utilizado somente impressões de matrizes para os alunos decodificarem em seus cadernos e a identificação dos caracteres e a matriz principal (matriz “chave”) para juntar com a matriz dada no papel foram colocados na lousa para que os discentes pudessem trocar os números das matrizes descobertos na sua resolução pelas letras e pontos colocados na lousa.

Antes da aplicação do jogo, os alunos tiveram um embasamento dado pelo professor de matemática e no dia da aplicação foi feita uma breve revisão de como resolver matrizes, principalmente multiplicação de matrizes e matrizes inversas e, ainda, eles aprenderam a importância e o uso na tecnologia de matrizes e toda a sua história do início das guerras, que foi primordial para o seu desfecho, até hoje, bastante utilizados em uso ainda de codificação e decodificação para a segurança das pessoas.

Diante disso, no jogo foi utilizado um método bastante simples que envolve matrizes inversas. Sejam A e B, tal que B é a matriz inversa de A.

$$A=\begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \qquad B=\begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$$

Logo podemos verificar que A*B = B*A = 1.

Vamos utilizar essas duas matrizes como “chaves” para codificar e decodificar a mensagem. O remetente vai usar a matriz A para codificar a mensagem e o destinatário vai usar a matriz B para decodificar a mensagem.

Para codificar uma mensagem o primeiro passo é convertê-la da forma alfabética para uma forma numérica. Então vamos utilizar a tabela abaixo (mas pode ser utilizada outras tabelas para dificultar a criptografia):

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10

K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20

U	V	W	X	Y	Z	.	!	#	Espaço
21	22	23	24	25	26	27	28	29	30

Antes da aplicação do jogo, ainda foi explicado como fazer e ainda foi feito exemplos para que os alunos pudessem tentar fazer sozinhos ou com a ajuda entre eles mesmos.

RESULTADOS E DISCUSSÃO

De início, foi explanado aos alunos a utilização das criptografias em tempos de Guerras. Cada aluno recebeu uma matriz codificada e uma "matriz-chave" que revelava a mensagem quando multiplicada e correlacionada a tabela. Foi notória certas dificuldades dos alunos devido a extensão das matrizes que deveriam calcular, no entanto houve auxílio por parte das bolsistas que foram explicando o passo a passo de como deveriam fazer.

Foi notória a empolgação e aceitação dos alunos com a atividade trazida em sala e com a devolutiva positiva deram a ideia de ser feita senhas com outras temáticas além de filmes. Conforme os alunos iam desvendando os filmes pelas dicas que encontravam, iam pegando outras matrizes para decodificar e também ajudar outros colegas que estavam tendo maior dificuldade. Eles conseguiram assimilar a importância de saber matrizes de forma divertida e descontraída.

Os discentes descobriram os códigos resolvendo as matrizes dadas e substituíram os números pelos caracteres, com isso encontraram uma pista de um filme e solucionaram o problema.

Foi bastante empolgante na parte de tentarem solucionar qual era o filme, e aí eles não podiam falar aos outros que ainda não tiveram descoberto o código e criou uma situação onde eles puderam brincar uns com os outros para "esconder" a dica que descobriram até que todos descobrissem. No final foi colocado na lousa todos os filmes que foram descobertos e aí eles puderam falar se acertaram ou não.

Pudemos observar também que os alunos que souberam resolver ajudaram uns aos outros para que todos conseguissem resolver pelo menos uma matriz e aprender, de forma lúdica, como resolver uma matriz. Outros alunos que terminaram rapidamente foram trocando os papéis para que pudessem resolver mais e descobrir mais dicas de filmes para que pudessem solucionar o problema colocado no código da matriz resolvida.

Ademais, os alunos se sentiram bastante empolgados e especiais por terem aprendido essa matéria, tendo em vista que esta foi e ainda é utilizada para decodificação e codificação de códigos bastante utilizados com a tecnologia que temos hoje, alguns até afloraram a ideia de querer ser da área de computação para conseguir criar programas que utilizasse matrizes.

CONSIDERAÇÕES FINAIS

Tendo em vista os feitos referidos, o uso da criptografia é corriqueiro no cotidiano, o uso da tecnologia nos faz ter um certo cuidado, pois há informações, por exemplo, dados pessoais, circulando na rede. Por isso, foi de suma importância o conhecimento sobre criptografia e criptoanálise para o entendimento dos alunos pois é do interesse deles para compreender o que está por detrás da ciência.

Além disso, os discentes puderam compreender que o uso de matrizes é extremamente relevante na tecnologia e que o conhecimento sobre os códigos utilizados nas guerras é somente uma introdução perto do que já foi descoberto com a uso de matrizes, como por exempli a decodificação de mensagens utilizadas em aplicativos, como o *Whatssapp* bastante utilizado por eles.

REFERÊNCIAS

Ibrahim A. Al-Kadit (1992): **ORIGINS OF CRYPTOLOGY: THE ARAB CONTRIBUTIONS**, Cryptologia, 16:2, 97-126.

História da criptografia. Disponível em <http://www.gta.ufrj.br/grad/07_1/ass-dig/HistriadaCriptografia.html > Acesso em: 15 de agosto de 2019.

A história da criptografia. Disponível em <http://www.dsc.ufcg.edu.br/~pet/jornal/abril2014/materias/historia_da_computacao.html> Acesso em: 21 de novembro de 2018.

BARBOSA, Sandra Lucia. **Jogos Matemáticos como Metodologia de Ensino Aprendizagem das Operações com Números Inteiros**. Disponível em <http://www.pucrs.br/famat/viali/tic_literatura/jogos/1948-8.pdf>

BORIN, J. **Jogos e resolução de problemas: uma estratégia para as aulas de matemática**. 3.ed. São Paulo: IME/USP, 1998.

SIQUEIRA, Regiane. **Tendências da Educação Matemática na Formação de Professores**. Disponível em <http://www.educadores.diaadia.pr.gov.br/arquivos/File/2010/artigos_teses/MATEMATICA/Monografia_regiane.pdf>

Uma breve história sobre Criptografia. Disponível em <https://cryptoid.com.br/banco-de-noticias/a-historia-da-criptografia/> Acesso em: 15 de agosto de 2019.