ESTUDO DA ARITMÉTICA MODULAR: JOGO CAÇA AO TESOURO

Sumaia Almeida Ramos [1,2]; Diana de Souza Carvalho[2, 3]; Severino Cirino de Lima Neto [4,5]

Professora da Rede Estadual de Pernambuco, lotada na Gerência Regional de Ensino Sertão do Médio São Francisco [(1)], membro do Núcleo de Pesquisa e Ensino em Matemática (NUPEMAT/UNIVASF) [(2)], sumaiaramos.math@gmail.com; Professora da Rede Estadual da Paraíba, lotada na Gerência Regional 01[(3)], membro do Núcleo de Pesquisa e Ensino em Matemática (NUPEMAT/UNIVASF), dianasous@gmail.com
Docente permanente do Programa de Mestrado Profissional em Matemática em Rene Nacional PROFMAT/UNIVASF, docente do Colegiado de Engenharia Mecânica da Universidade Federal do Vale do São Francisco [(4)] e Coordenador do Núcleo de Pesquisa e Ensino em Matemática (NUPEMAT/UNIVASF) [(5)], cirino.univasf@gmail.com

Resumo: Um desafio da educação no século XXI é definir uma didática que atenda as expectativas dos estudantes, considerados nativos digitais e apreciadores de ambientes gamificados, para uma educação que estimule a aprendizagem e de forma divertida. Com isso, essa proposta tem como objetivo analisar a viabilidade do jogo Caça ao Tesouro como uma ferramenta de ensino capaz de promover um ambiente de aprendizagem significativa. Para isso, a metodologia se dividiu em quatro momentos: 1) exposição de conteúdo; 2) debate com tema transversal; 3) aplicação do jogo; e. 4) aplicação de questionário. Os dados revelam que 97% do público-alvo considera o jogo divertido e capaz de auxiliar na aprendizagem, promovendo um ambiente de aprendizagem significativa, além de promover a autonomia do estudante. Além disso, a ferramenta mostrou-se possível de ser utilizada por professores de diversas disciplinas, sendo necessárias apenas algumas adaptações simples durante o planejamento, no entanto em alguns casos será importante utilizar o auxilio de um software capaz de cifrar e decifrar mensagens.

Palavras-chave: Gamificação, aritmética modular, jogos, aprendizagem significativa.

Introdução

No cenário da Segunda Guerra Mundial, um dos maiores inventos da inteligência artificial estava sendo criado: a Máquina de Turing (STRATHERN, 2000). Este invento impulsionou a criação das tecnologias modernas, acelerando as mudanças sociais e tecnológicas no mundo. Entretanto, é a partir da década de 1970 que as mudanças mundiais ganham velocidade em consequência da possibilidade de troca de mensagens por computadores e linhas telefônicas, criando, a partir da década de 1980, os nativos digitais (PALFREY; GASSER, 2011).

Isso permite afirmar que as salas de aula da educação básica do século XXI são formadas por nativos digitais, desafiando a educação a ofertar de um ambiente de aprendizagem que se concatenem com as características deste público. Por conseguinte, as academias de licenciatura devem investir em pesquisas com práticas inovadoras, afim de moldar uma didática que atenda à esta era tecnológica.

Uma das características dos nativos digitais é o uso de games digitais, atividade que ocupa a maior parte do dia produtivo desse grupo. Em 2013, nos EUA, a maior parte das residências possuía pelo menos um dispositivo com capacidade para rodar games; no Brasil,

cerca de 23% do público jovem era jogador assíduo ou casual, o que correspondia a cerca de 45 milhões de jogadores. Esses dados são refletidos em sala de aula, em que os adolescentes estão equipados com aparelhos móveis cada vez mais sofisticados e considerados indispensáveis em contexto social, provocando os educadores a buscar formas de usar essa ferramenta no processo de aprendizagem.

Pesquisas publicadas recentemente apresentam resultados positivos em relação a uma nova prática pedagógica chamada gamificação, que consiste na utilização de elementos dos games fora do seu contexto (FARDO, 2013; SILVA et al, 2018). Tal prática pode ser usada em sala de aula, favorecendo melhor participação dos estudantes nas atividades propostas pelo professor.

Para contribuir com as pesquisas já publicadas sobre a viabilidade do uso de jogos na educação, esta pesquisa propôs o uso da gamificação no ensino da matemática, tendo como foco o estudo da aritmética modular aplicada à criptografia. Como uma forma de gamificar o ambiente de aprendizagem, o objetivo foi analisar a viabilidade do jogo Caça ao Tesouro como uma ferramenta de ensino capaz de promover um ambiente de aprendizagem significativa e transdisciplinar.

Metodologia:

A atividade foi aplicada em formato de oficina com o objetivo de analisar a viabilidade do uso do jogo Caça ao Tesouro como ferramenta de aprendizagem. Para tanto, uma das etapas da atividade é a aplicação de um questionário que possibilite uma análise sobre a opinião dos participantes. Aplicada em uma turma de 45 (quarenta e cinco) estudantes das escolas públicas de Petrolina – PE (público desta proposta), dos anos finais (6º ao 9º ano) do ensino fundamental, teve como objetivo levantar dados que possibilitem inferir a eficiência da proposta, descrevendo as dificuldades encontradas pelos sujeitos e as vantagens da aplicação.

A metodologia desta proposta está dividia em quatro momentos: 1) Exposição do conteúdo: momento que o professor apresenta os conceitos de aritmética modular aplicada a criptografias primitivas; 2) debate com tema transversal: conversa sobre os impactos ambientais sofridos pelo rio São Francisco[3]; 3) aplicação do jogo: neste momento os estudantes participaram do jogo que exige conhecimento de conceitos discutidos nos momento anteriores; 4) aplicação de questionário: destinado a avaliar opinião dos estudantes sobre o uso do jogo para fundamentação da proposta.

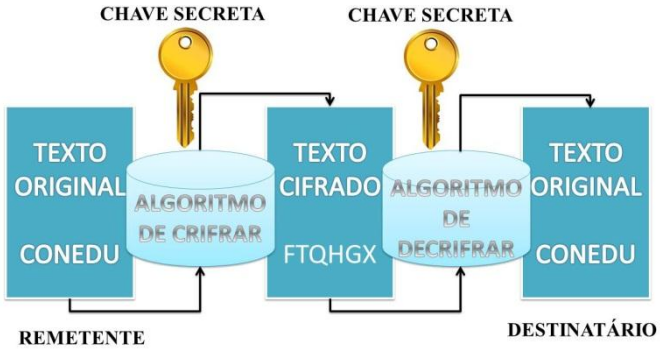
Os estudantes vivenciaram um jogo que exige dos jogadores conhecimentos sobre os conceitos de aritmética modular aplicada à criptografia, além de permitir uma reflexão crítica sobre problemas ambientais que o cercam. Em cada jogada, foi proposto uma reflexão e crítica aos atuais problemas enfrentado pelo rio São Francisco.

Resultados e Discussão

A exposição teórica dos conceitos de aritmética modular, realizada no primeiro momento da sequência didática, foi trabalhada aplicada a criptografias primitivas, sendo usada apenas a cifras de substituição de César e afim.

Essas criptografias só são possíveis após a escolha de uma chave secreta que deverá ser compartilhada entre o destinatário e o remetente. O processo de criptografar consiste em usar a chave secreta no texto original modificando a identidade das letras, sendo sua leitura possível apenas para quem possuir a chave (figura 1).

Figura 1: Processo de criptografia: criptografar e decifrar



Fonte: Próprio autor

CIFRA DE CÉSAR

Considerada uma das cifras mais antigas, foi utilizada pelo Imperador Júlio César na Roma Antiga. O seu processo se baseava em substituir letras do texto original por letras de um alfabeto cifrado. Para isso, atribui-se valores numéricos ao alfabeto de 26 letras (tabela 1) Malagutti (2015), Shokranian (2012) e Singh (2002).

Tabela 1: Alfabeto utilizado na Cifra de César

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Próprio autor

Considerando y o valor da letra do texto cifrado e x o valor da letra do texto original, o algoritmo de cifrar utilizado por César é $y = x + chave$. A chave deve ser compartilhada com segurança. Quando a soma gerar um valor maior que 25, é aplicado a congruência modular $y \equiv x + chave\ mod\ 26$ (SHOKRANIAN, 2012).

Suponha que o texto original seja CONEDU, utilizando chave 3 o texto cifrado será FTQHGX, pois veja que o texto original será substituído pelos números $2 - 16 - 13 - 4 - 3 - 20$, aplicando no algoritmo de cifrar a primeira letra será $y = 2 + 3 = 5 = F$, em seguida $y = 16 + 3 = 19 = T$ e a assim sucessivamente.

Para decifrar o remetente deve ter posse da chave secreta e aplicar a operação inversa $x = y - chave$ ou $x \equiv y - chave\ mod\ 26$. Logo, ao receber a mensagem cifrada FTQHGX, de acordo com a tabela 1, a representação numérica será $5 - 19 - 16 - 7 - 6 - 23$. Aplicando no algoritmo de decifrar a primeira letra será $x = 5 - 3 = 2 = C$, em seguida $x = 19 - 3 = 16 = O$ e assim sucessivamente. Quando necessário deve-se aplicar a congruência módulo 26.

Alguns autores como Malagutti (2015), Shokranian (2012) e Singh (2002), afirmam que a Cifra de César é um caso particular da cifra afim. Sendo considera uma cifra com duas chaves a e b, com $a = 1\ e\ b \in \mathbb{Z}^*$ tal que $y = ax + b$.

CIFRA AFIM

O algoritmo da cifra afim funciona com duas chaves a e b, com $a \in Z_{|26|}$ e $b \in \mathbb{Z}^*$, tal que $y \equiv ax + b\ mod\ 26$. A necessidade de da chave a pertencer ao conjunto dos inversos modulo 26 está na possibilidade de realizar a operação inversa no ato de decifrar, tal que para isso faz-se $(y - b)a^{-1} \equiv x\ mod\ 26$. Logo, a só pode ser um dos restos possíveis na divisão por 26 (MALAGUTTI, 2015); (SHOKRANIAN, 2012).

Observe que ao cifrar a mensagem CONEDU com a cifra afim de chaves $a = 10\ e\ b = 23$, o algoritmo será $y \equiv 10x + 23\ mod\ 26$. Logo, aplicando na letra C de valor numérico 2, tem-se $y \equiv 10 \cdot 2 + 23 = 43 \equiv 17\ mod\ 26$, daí C deve ser substituída por R, porém para decifrar a operação inversa a ser aplicada será $(17 - 23) \cdot 10^{-1} \equiv x\ mod\ 26$.

Tabela 2: Inversos modulares de Z_{26}

Resíduos	1	3	5	7	9	11	15	17	19	21	23	25
Inversos modulares	1	9	21	15	3	19	7	23	11	5	17	25

Fonte: Próprio autor.

De acordo com a tabela 2, o número 10 não possui inverso módulo 26, não sendo possível realizar a operação inversa, ou seja a escolha dessas chaves só permite cifrar. Trocando a chave $a = 10$ por $a = 3$, a letra C será cifrada por D, pois $y \equiv 3 \cdot 2 + 23 = 29 \equiv 3 \; mod \; 26$. Para decifrar seguira o processo inverso $(3 - 23) \cdot \mathbf{3^{-1}} \equiv x \; mod \; 26$, como o inverso de 3 modulo 26 é o 9, tem-se $-20 \cdot \mathbf{9} \equiv x \; mod \; 26$, o que implica $-180 \equiv 2 \equiv x \; mod \; 26$, ou seja -180 deixa resto 2 ao ser dividido por 26.

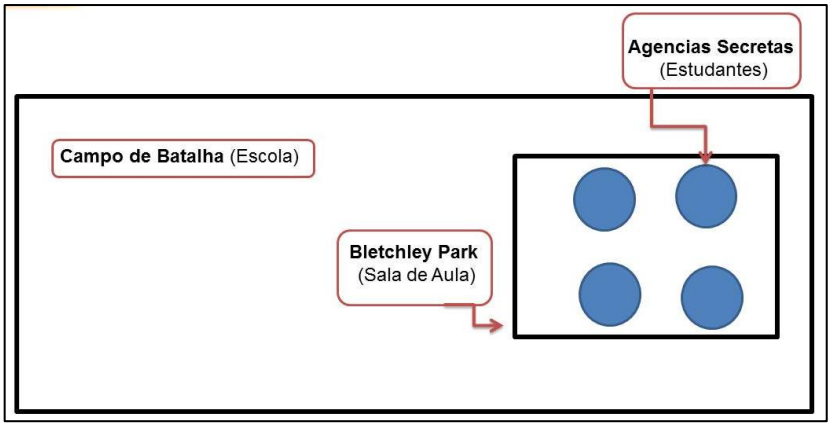
JOGO CAÇA AO TESOURO

O jogo Caça ao Tesouro foi criado como parte da dissertação do Mestrado Profissional em Rede Nacional (PROFMAT/UNIVASF), com objetivo de estimular a aprendizagem de matemática de forma divertia, além disso, sua estrutura foi pensada com a preocupação de deixar o mais próximo possível da realidade do uso de criptografias com a ideia de proteção de informações sigilosas. A ideia é que durante o jogo, o estudante seja capaz de aplicar os conhecimentos abordados durante as aulas; neste âmbito, se trata de uma ferramenta de auxilio na fixação dos conceitos estudados.

Para a realização do jogo, pensou-se em um cenário que pode ser criado na imaginação da criança, influenciada pelos nomes dados ao ambiente. Geralmente, o ambiente físico a ser utilizado é a escola, onde a sala de aula recebe o nome de *Bletchley Park* , esse nome é em homenagem ao local onde o matemático Alan Turing decifrou a Enigma durante a Segunda Guerra Mundial, na Inglaterra.

Na sala de aula, os estudantes devem ser divididos em grupos, na qual cada um será uma agencia secreta. Os grupos são identificados com nomes que podem ser escolhidos pelos próprios integrantes. Em cada agência, deve ser indicado quem será o líder, os criptógrafos e criptoanalistas. O líder será o intermediário entre o juiz (professor) e sua agência secreta (figura 2).

Figura 2: Ilustração do cenário do jogo Caça ao Tesouro.



Fonte: Próprio autor.

O objetivo principal do jogo é encontrar um tesouro perdido. Para isso, as agências vão em busca de pergaminhos que os direcionará ao pergaminho seguinte. O jogo finaliza quando uma das equipes encontrar o tesouro. No entanto, para conseguir realizar a leitura da mensagem contida em cada pergaminho, os agentes devem decifrar a mensagem e, por meio dela, tentar identificar onde encontrar o próximo pergaminho.

Como já se sabe, para decifrar a mensagem é necessário conhecer a cifra utilizada e a chave. Com isso, em cada pergaminho estar especificada a cifra que foi utilizada, por outro lado, a chave é a solução de uma questão de matemática solucionada no *Bletchley Park.* Isto é, o jogo inicia com uma questão relacionada ao conteúdo que se deseja revisar, a solução será a chave para decifrar o pergaminho.

Cada pergaminho foi produzido em quantidade igual ao das equipes, assim o Juiz inicia o jogo entregando para cada líder o pergaminho referente à primeira pista, que vai informar onde está localizado o pergaminho 2. Cada agencia indicará dois integrantes para procurar o pergaminho, que só serão liberados para a caça ao pergaminho quando a agência decifrar a solução para o pergaminho que está em análise.

Enquanto os agentes estão procurando o pergaminho, o juiz já expõe na lousa a questão que contem a chave do pergaminho três, assim as agencias vão tentando solucionar enquanto chega à informação com a localização encontrada. A primeira equipe que encontrar o pergaminho deve retornar para sua agencia onde deverá decifrar a mensagem. Após a leitura e em posse da chave do pergaminho 3, a agencia deve enviar dois agentes em busca da nova pista, no entanto, não poderão ser os mesmos da jogada anterior, ou seja, dois estudantes, nunca vão em busca de um pergaminho em jogadas consecutivas. Essas jogadas se repetem até ser encontrado o último pergaminho.

Figura 3: Ilustração de um dos pergaminhos. (a) Cifrado; (b) Decifrado

(a)

(b)

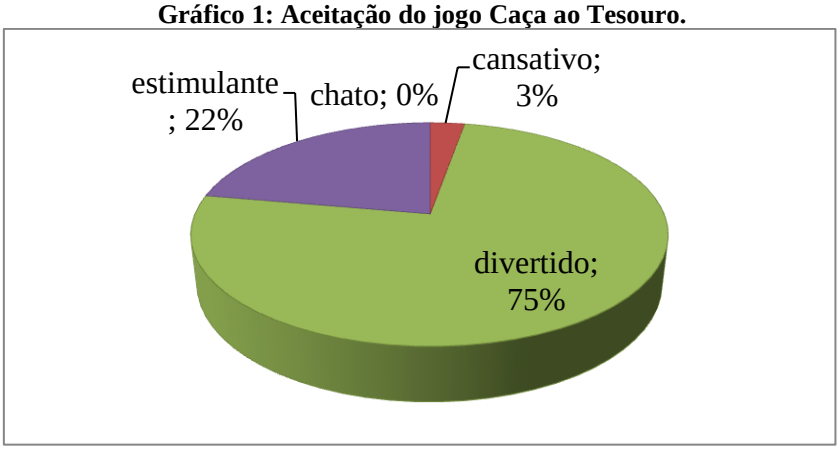
Fonte: Próprio autor

Note que se trata de um jogo interativo, onde todos participam das jogadas, permitindo uma interação dentro das equipes. O que chama a atenção na aplicação do jogo é a participação voluntária de todos e o companheirismo. Aqueles que apresentavam mais dificuldade para cifrar e aplicar os conceitos estudados participavam de discussões com os colegas que apresentavam mais habilidades nessa atividade.

Antes da aplicação do jogo, foi realizada uma discussão inicial sobre a importância do Rio São Francisco para as cidades de Juazeiro-BA e Petrolina-PE e os atuais problemas relacionado ao mau uso de suas águas, bem como a urbanização como fator que contribui para erosão e eutrofização de suas águas. Com isso, os pergaminhos foram elaborados com mensagens que refletiram a discussão realizada sobre os impactos ambientais sofridos pelo rio.

Com o objetivo de avaliar a eficiência do jogo, além da observação realizada pelo professor, aplicou-se um questionário. A primeira questão questionava ao estudante se este considera o jogo Caça ao Tesouro um jogo chato, cansativo, divertido ou estimulante. Observou-se que 87% dos estudantes demonstraram uma boa aceitação do jogo, de tal forma que 75%, afirmaram ser um jogo divertido e 22% consideraram estimulante (gráfico 1). Esta é uma característica fundamental dos jogos: a participação voluntária é estimulada pelo prazer sentido em participar do jogo. Este prazer pode ser estimulado pelos desafios apresentados durante o jogo e pela sensação de ser capaz de competir (LIMA, 2008).

Gráfico 1: Aceitação do jogo Caça ao Tesouro.

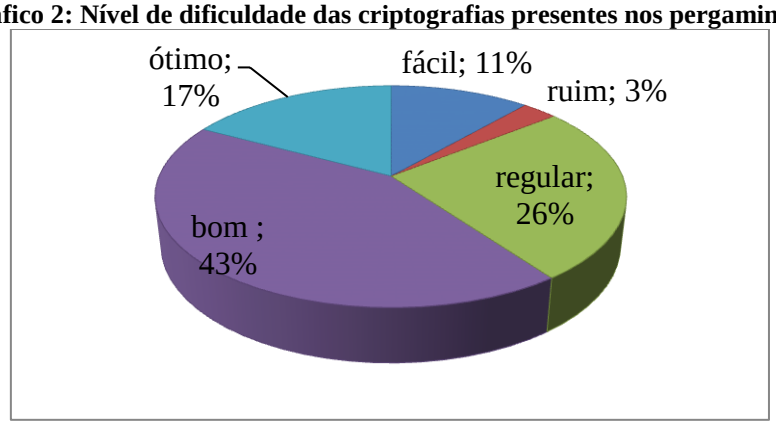


Fonte: Próprio autor.

A segunda questão tem como objetivo identificar, a partir da opinião dos estudantes, as dificuldades presentes nas criptografias dos pergaminhos. Quanto ao nível de dificuldade das criptografias presentes nos pergaminhos, 11% dos estudantes consideraram fácil, 17% ótimo e 43% bom; apenas 29% dos estudantes afirmaram ser ruim ou regular. Por meio da terceira questão, 91 % dos estudantes afirmaram que o jogo contribuiu de forma positiva na

sua aprendizagem, permitindo fixar de forma significativa o conteúdo trabalhado, facilitando a assimilação dos conceitos durante a experiência.

Gráfico 2: Nível de dificuldade das criptografias presentes nos pergaminhos.



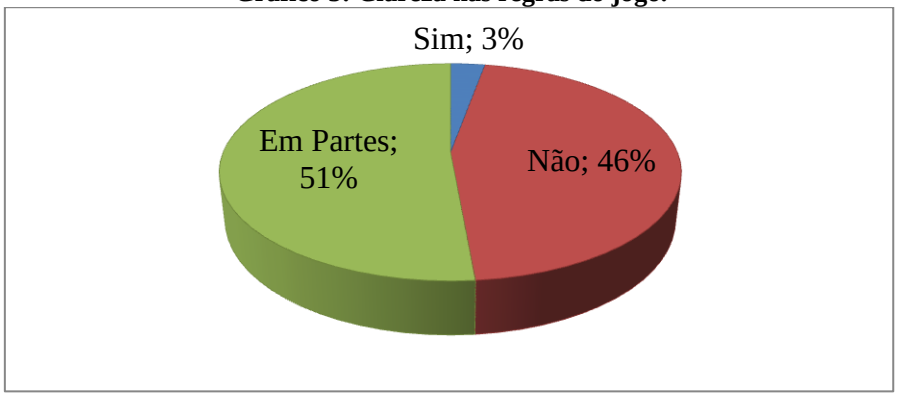
Fonte: Próprio autor.

Identificar se houve algum tipo de aprendizagem na aplicação do jogo é uma forma de avaliar se é possível considera-lo um jogo educativo. Durante as jogadas, a observação na interação dos estudantes permitiu perceber nas equipes com oito estudantes cerca de 4 a 5 integrantes dominavam o conceito, e os demais apresentavam dificuldades distintas, alguns durante as cifras outros durante as soluções das questões.

No entanto, a aprendizagem não ocorre apenas quando o aluno chega a um resultado correto. A partir do momento em que o estudante consegue chegar a uma tese, o professor deve ajuda-lo a identificar se é válida ou não. Não sendo válido, o estudo e as análises serão feitos sobre o erro que tornou a tese inválida de modo a torna-la válida.

A quarta questão tem como objetivo identificar se as regras do jogo estão bem definidas e claras para os estudantes, na qual apenas 3% afirmaram sentir dificuldades em compreender as regra. Tal dificuldade pode ter sido gerada pela falta de leitura do regulamento, ou pela falta de atenção durante as explicações, uma vez que mais de 90% dos estudantes compreenderam as regras estabelecidas.

Gráfico 3: Clareza nas regras do jogo.



Fonte: Próprio autor.

Desta forma, estes dados permitem concluir que o jogo, quando bem planejado, oferece várias possibilidades, uma vez que o próprio estudante é quem realiza os cálculos, já que encontrar o resultado é fundamental para progredir no jogo, desenvolvendo assim a autonomia, levando em consideração que eles levantam hipótese, testam os cálculos e chegam a uma tese.

Conclusões

Apesar da proposta está direcionada ao ensino da matemática, ao interagir com o tema transversal meio ambiente, além de ser uma exigência dos PCN, é uma forma de mostrar que o Caça ao Tesouro pode ser adaptado a qualquer disciplina, basta modificar as mensagens dos pergaminhos que podem ser feitas com a ajuda do programa de criptografia, e as questões com as soluções das chaves podem ser substituídas por aquelas direcionadas à disciplina.

É importante salientar que, se o professor de outra disciplina decidir utilizar do jogo como auxilio na revisão de seus conteúdos, mas não apresentar para o estudante os conceitos de criptografia, haverá uma necessidade de utilizar algum programa de criptografia como ferramenta do jogo, optando pelas cifras mais simples, mas fazendo uma exposição bem geral de como ocorre o processo da escolha da chave. Caso contrário, o estudante não conseguirá participar do jogo, levando-o à desistência e à recusa em fazer parte da atividade.

Pensando nisso, esse trabalho fundamenta uma pesquisa de Iniciação Cientifica Junior que tem como objetivo programar um aplicativo de multiplataformas para auxiliar professores de outras disciplinas no uso do Caça ao Tesouro como ferramenta de ensino. Tal pesquisa ainda está em andamento.

Referências:

FARDO, Marcelo Luiz. **A gamificação aplicada em ambientes de aprendizagem.** Revista Novas Tecnologias na Educação. v. 11, n 1, jul 2013. Disponível em: < http://seer.ufrgs.br/renote/article/view/41629/26409>. Acesso em: 20 ago de 2018.

LIMA, J. M. **O jogo como recurso pedagógico no contexto educacional.** São Paulo: Cultura Acadêmica: Universidade Estadual de Paulista, Pró reitoria de Educação, 2008.

MALAGUTTI, P. **Atividades de contagem a partir da criptografia.** Rio de Janeiro, IMPA, 2015. 77p.

PALFREY, John; GASSER, Urs. **Nascidos na era digital:** entendendo a primeira geração de nativos digitais. Porto Alegre: grupo a, 2011.

SILVA, João Batista da; ANDRADE, Maria Helena; et al. **Tecnologias digitais e metodologias ativas na escola: o contributo do kahoot para gamificar a sala e aula.** Revista Thema. v. 15, n 2, p. 780-791, 2018. Disponível em: file:///C:/Users/User/Documents/PROJETOS%20DE%20MATEM%C3%81TICA/ARTIGOS/CONEDU/2018/REFER%C3%8ANCIAS/838-3974-1-PB%20_%202018.pdf. Acesso em: 01 set de 2018.

SHOKRANIAN, Salahoddin. **Criptografia para iniciantes.** 2.ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2012.

SINGH, S. **O livro dos códigos**. Tradução de Jorge Calife. 2.ed. Rio de Janeiro: Record, 2002.

STRATHERN, P. **Turing e o computador em 90 minutos**. Traduzido por Mara Luiza X. de A. Borges. Jorge Zahar Editor. 2000.