UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

EWELLYN AMÂNCIO ARAÚJO BARBOSA

O USO DO RPG PARA A APRENDIZAGEM DE CRIPTOGRAFIA

Maceió
2020

UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE MATEMÁTICA
CURSO DE LICENCIATURA EM MATEMÁTICA

EWELLYN AMÂNCIO ARAÚJO BARBOSA

R.A: 16110297

O USO DO RPG PARA A APRENDIZAGEM DE CRIPTOGRAFIA

Trabalho de Conclusão de Curso apresentado para o Instituto de Matemática.

Orientadora: Profª. Me. Elisa Fonseca Sena e Silva.

Maceió
2020

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 – 1767

B238 Barbosa, Ewellyn Amâncio Araújo.
O uso do RPG para a aprendizagem de criptografia / Ewellyn Amâncio Araújo Barbosa. - 2020.
56 f. : il. color.

Orientadora: Elisa Fonseca Sena e Silva.
Monografia (Trabalho de Conclusão de Curso em Matemática : Licenciatura) – Universidade Federal de Alagoas. Instituto de Matemática. Maceió, 2020.

Bibliografia: f. 46-47.
Apêndice: f. 48-56.

1. Criptografia. 2. Jogos de fantasia. 3. Aprendizagem. 4. Teoria dos números. 5. Ensino básico. I. Título.

CDU: 372.851:371.695

FOLHA DE APROVAÇÃO

EWELLYN AMÂNCIO ARAÚJO BARBOSA

O USO DO RPG PARA A APRENDIZAGEM DE CRIPTOGRAFIA

Monografia submetida ao corpo docente do curso de Matemática da Universidade Federal de Alagoas em 21 de maio de 2020.

Profª. Me. Elisa Fonseca Sena e Silva (Orientadora)
Universidade Federal de Alagoas – UFAL

BANCA EXAMINADORA:

Profª. Dra. Viviane de Oliveira Santos
Universidade Federal de Alagoas – UFAL

Profª. Dra. Juliana Roberta Theodoro de Lima
Universidade Federal de Alagoas – UFAL

UNIVERSIDADE FEDERAL DE ALAGOAS
INSTITUTO DE MATEMÁTICA
COORDENAÇÃO DO CURSO DEMATEMÁTICA LICENCIATURA
Fone: 3214-1405 / E-mail: coordenacao.matl@im.ufal.br

DECLARAÇÃO DE NOTA DE TCC

Informamos à Coordenação do Curso de Graduação em Matemática Licenciatura que o Trabalho de Conclusão de Curso do(a) aluno(a) **EWELLYN AMÂNCIO ARAÚJO BARBOSA**, matrícula nº **16110297**, do curso de **MATEMÁTICA LICENCIATURA**, intitulado: "**O uso do RGP para a aprendizagem de criptografia**", recebeu da Banca Examinadora a seguinte nota: **9,0** (nove), média obtida a partir das seguintes notas atribuídas pelos componentes da Banca Examinadora:

Profa. Elisa Fonseca Sena e Silva (Orientadora): 9,0
Profa. Viviane de Oliveira Santos: 9,0
Profa. Juliana Roberta Theodoro de Lima: **9,0**

Maceió, 21 de maio de 2020.

Profa. Elisa Fonseca Sena e Silva

Profa. Viviane de Oliveira Santos

Profa. Juliana Roberta Theodoro de Lima

Dedico este trabalho ao meu Deus, a Ele toda honra e glória. Tu és meu fiel companheiro, amigo, pai e consolador nos momentos difíceis, que me guiou ao longo desses quatro anos e mostrou a cada dia o valor de seu inestimável carinho e amor incomparável. Os céus proclamam a sua glória Senhor e o firmamento anuncia a obra das suas mãos. A Ti, ofereço todo o meu ser.

AGRADECIMENTOS

Agradeço a Deus, por ter me ajudado em todos os momentos, sendo meu alicerce e me abençoando com sabedoria e infinita bondade durante todo este curso.

Aos meus pais, por terem me ensinado valores e princípios que guardarei por toda vida. Mainha, obrigada por todo cuidado e paciência mesmo com todas as dificuldades. Painho, obrigada pela confiança e por acreditar no meu sucesso. Amo vocês!

A toda minha família, por estarem comigo sempre que precisei, às minhas irmãs Mili e Bequinha, minha vózinha obrigada por tanto, Weslley, Jane, Titia, Glorinha, Vô Agapito, Jailton, RJ. Gratidão a todos.

Ao PET C&T, programa incrível que me proporcionou momentos únicos e convivência com pessoas que marcaram minha vida como estudante e ser humano. Iany, Feijãozinho, Dani, Sandrelena Madalena, Fernandinha por todas as massagens em minha mão e por ser fofinha mesmo com todas as patadas, Mary, May, Adris e a todos os meus amigos do PET que fizeram parte dessa jornada. Eu amo vocês.

A todos os meus amigos, Andressa, Yané, meus *migles* da igreja e aos de sempre, Hadassa que se fez presente em todos os meus momentos. Ao meu amigo Magão, por sempre me acordar com um bom dia e perguntar como estou. Vocês me fazem bem, *Je t'aime*.

Ao Instituto de Matemática que me presenteou com professores essenciais para minha formação, que se preocupam não apenas em lecionar, mas com o futuro e bem estar dos alunos, Juliana, Viviane, Isadora, Elisa, Cláudia, Davi, Isnaldo, Tiarlos, Karenzinha, além dos amigos que guardarei em meu coração e a todos que contribuíram de alguma forma, obrigada.

Agradeço à minha orientadora Elisa Sena, um exemplo de mulher e professora, obrigada por toda paciência e dedicação.

Ao professor Roberaldo Carvalho, que me orientou, me apresentou o PAESPE e compartilhou suas experiências. Obrigada por sair da sua zona de conforto e transformar vidas através da educação. Também agradeço à Geiza por seu cuidado e amor ao PAESPE.

Ao tutor Eduardo Lucena, por sua horizontalidade, empatia e paciência com nosso grupo.

Por fim, agradeço ao Fernandinho, por todo companheirismo, amor, afeto, paciência e carinho, você é um presente de Deus pra mim. Amo-te.

Obrigada a todos que participaram diretamente ou indiretamente para a realização desse trabalho!

“Para conseguir o que quer, você deve olhar além
do que você vê.”

Filme O Rei Leão 3

RESUMO

Neste trabalho foram mostrados, por meio de pesquisas bibliográficas e materiais desenvolvidos, métodos de como se ensinar criptografia aliada aos conhecimentos de teoria dos números com o uso do *Roleplaying Game* (RPG) como ferramenta pedagógica. Foi incluído o relato de uma aplicação realizada com alunos do Ensino Médio inseridos no Programa de Apoio aos Estudantes de Escola Pública do Estado (Paespe) da Universidade Federal de Alagoas (Ufal). O uso do RPG como ferramenta pedagógica vem sendo utilizado ou sugerido em diversos trabalhos e pode ser unido a diversas disciplinas escolares, como a matemática, possibilitando que ela seja inserida de maneira leve e eficaz no processo de aprendizagem dos alunos. A criptografia fornece códigos secretos para determinada mensagem ser mantida em segredo para que apenas o destinatário desejado possa ter acesso à mesma. Os avanços tecnológicos no mundo demandaram métodos mais seguros para se proteger uma mensagem, dentre esses métodos a criptografia RSA (cuja sigla vem da inicial de seus criadores) recebe um destaque, por utilizar uma ideia matemática relativamente simples em seu processo de codificação, porém com um nível enorme de dificuldade para poder ser decodificada. Para utilizar as ideias da criptografia RSA, é preciso ter alguns conhecimentos de teoria dos números. Ao todo, participaram da aplicação do RPG educacional, conhecido também como RPG pedagógico, setenta e quatro alunos e três professoras voluntárias do programa incluindo a autora deste trabalho. O planejamento foi feito visando analisar o interesse dos alunos com metodologias diferenciadas e utilizar os conhecimentos teóricos sobre as diversas formas de criptografia, incluindo os conhecimentos de teoria dos números. Os resultados obtidos demonstram que a utilização do jogo e do conteúdo escolhido, junto com a maneira interdisciplinar que foi proposta a aventura, permitem que o aluno possa participar efetivamente e fixar melhor o conteúdo dado teoricamente, aproximando os estudantes da matemática, quebrando os receios e fazendo com que eles enxerguem no sentido do que foram ensinados. Também se observou a união dos alunos para superar os desafios e o diálogo presentes antes de cada ação solicitada.

Palavras-chave: Criptografia. RPG. Aprendizagem. Teoria dos números. Ensino básico.

ABSTRACT

In this paper, methods on how to teach cryptography and number theory were shown using Roleplaying Game as a pedagogical tool. A report on an activity executed with high school students included in the Support Program for Students from Public State Schools (PAESPE) from the Federal University of Alagoas (UFAL) was included. The usage of RPG as a pedagogical tool has been used or suggested by various papers and can be applied to various subjects, such as mathematics, enabling its insertion in the learning process effectively. Cryptography provides secret codes so that certain message can be kept in secret, thus only the addressee has access to it. Technological advances in the world demand safer methods to protect messages, within those methods RSA cryptography has been highlighted for using a relatively simple mathematical idea in its codification process without compromising the high security level for the decodification of the message. In order to use the ideas of the RSA cryptography, number theory knowledge is fundamental. Altogether, seventy four students and 3 volunteer teachers, including the author of this paper, participated on the execution of the pedagogical RPG experience. The planning was made keeping the students engagement in mind with various methodologies and using knowledge from several cryptography forms, including knowledge about number theory. The obtained results show that the usage of the game, considering the interdisciplinary way the adventure was proposed, allowed the students to participate and memorize effectively the theory previously presented. The union and dialogue within the students in order to solve the presented problems was also noted.

Key words: Cryptography. RPG. Learning. Number theory. Basic education.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Roleplaying Game, também conhecido como RPG, teve sua primeira publicação no ano de 1973, nos Estados Unidos sob o título DUNGEONS & DRAGONS. Desde a sua criação, o RPG é apresentado vinculado à literatura fantástica, visto que essa "primeira publicação tratava de uma fantasia medieval fundamentada no universo e aventuras da obra do escritor e professor de filologia de Oxford, J.R.R. Tolkien" (VASQUES, 2008, p. 12).

Desde alguns anos atrás existem discussões sobre o RPG aplicado na área educacional, podendo ser uma ferramenta didática simples e de baixo custo monetário ao alcance do professor. As pesquisas sobre o tema vêm tendo destaque no quesito pedagógico e a tendência é ter avanços e mais trabalhos que não comentem apenas teoricamente a possível aplicação do RPG em sala de aula, mas também registros de experiências práticas de professores que fizeram uso deste recurso como auxílio de aprendizagem, relatando as dificuldades e devolutivas da aplicação (AMARAL, 2013, p. 7).

Para a construção das aventuras do RPG pedagógico, o professor pode utilizar diversos assuntos que sejam da disciplina que ministra. Neste trabalho, o enfoque será a matemática, para torná-la interdisciplinar e divertida. O conteúdo de criptografia pode ser facilmente introduzido nas aventuras, que são basicamente histórias contadas no jogo, visto que é um tema amplo, contendo fatos históricos e está ligado à matemática em alguns de seus métodos, fazendo com que o aluno possa utilizar na prática os conhecimentos adquiridos em aulas teóricas, fixando melhor o que foi ensinado.

Para Oliveira (2015, p. 23), "Durante muitos anos, até os dias de hoje, inúmeros acontecimentos marcaram época e ficou gravado na história, a criptografia é um delas". A palavra criptografia deriva do grego Kryptós, "escondido", e gráphein, "escrita". (FIGUEIREDO, 2012, p. 44). A criptografia está presente no cotidiano dos alunos e é um conteúdo diferente para se trabalhar, pois os estudantes estão acostumados a ter uma matemática mecânica em que apenas realizam algumas contas e não conseguem compreender o que estão realizando.

A criptografia é um assunto que tem despertado interessante no contexto atual, sendo utilizado bastante em sala de aula. "Acredita-se que seu uso possa despertar um algo a mais nos alunos, motivando-os e ajudando o professor a contornar dificuldades ao tentar estimular seus estudantes no aprendizado e nos conceitos relacionados com o ensino da Matemática", (MACHADO, 1997, p. 95).

Um dos métodos de criptografia que utiliza técnicas presentes em teoria dos números em seu procedimento é a RSA, que é um dos métodos mais conhecidos de chave pública,

segundo Coutinho (2010, p. 9). “Este código foi criado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que trabalhavam no *Massachussets Institute of Technology* (M.I.T)”. As letras RSA correspondem às iniciais dos inventores.

Diante do que foi exposto, o presente trabalho tem o intuito de unir os conhecimentos dos diversos métodos de criptografia, inclusive a RSA, e utilizar o RPG pedagógico como ferramenta para o processo de aprendizagem no ensino básico, tendo foco também em mostrar ao professor como colocar em prática o RPG em sala de aula e conseguir experiências positivas e motivadoras.

Pretende-se apresentar ao professor, através da aplicação relatada neste trabalho, métodos e adaptações de como ensinar a criptografia para os alunos de maneira leve e dinâmica, e motivá-lo a utilizar a imaginação e criatividade para a criação das aventuras que serão a fonte principal de uma aplicação deste jogo. Segundo Amaral (2013, p. 8) “cada sala de aula é um universo diferente e você deverá encontrar a chave para abrir o baú que guarda os segredos de uma fantástica experiência do RPG na escola”.

Este trabalho de conclusão de curso está dividido em três capítulos: o primeiro aborda acerca da criptografia em seu percurso histórico e sobre a criptografia RSA, a qual faz uso de conceitos de teoria dos números, fundamentada em estudos sobre seu uso no ensino básico e estratégias metodológicas para uma melhor aprendizagem. O capítulo seguinte fala sobre o RPG em sala de aula e como pode ser introduzido, apresentando sua historicidade e como se joga, informando as regras de jogo e o objetivo final, além de apresentar pontos importantes de autores sobre seu uso na área da educação e em como ele pode motivar os alunos. No terceiro capítulo, serão finalmente apresentados os resultados da aplicação de RPG com o uso de criptografia, realizada com alunos da segunda série do Programa de Apoio aos Estudantes de Escola Pública do Estado (PAESPE) da Universidade Federal de Alagoas (Ufal). Ao fim do documento estão disponibilizados em anexo a aventura e o plano de aula informando seu o planejamento, para contribuir com o professor que desejar adaptar ou utilizar este método em sua disciplina ou sala de aula.

2 CRIPTOGRAFIA

A seguir, serão abordados três tópicos acerca da criptografia. Inicialmente será visto o ensino de criptografia, seu percurso histórico e por fim um estudo mais detalhado sobre a criptografia através método RSA.

2.1 Ensino de criptografia

A matemática no ensino básico é uma das disciplinas em que os discentes possuem mais dificuldades de aprendizagem, seja em relação à sua aplicação no cotidiano ou à forma com que o conteúdo é introduzido em sala de aula, dentre outros fatores. O professor que deseja ministrar suas aulas de modo que os alunos construam seus conhecimentos de forma significativa deve compreender que atualmente ministrar uma aula não significa ensinar somente fórmulas e realizar atividades mecânicas, mas sim buscar maneiras de como apresentar o conteúdo de modo que se consiga atingir o objetivo de que o aluno tenha um melhor desempenho, alcançando a compreensão do que for ensinado.

A escola é um ambiente que promove a educação, o convívio social e tem a função de buscar um desenvolvimento em conjunto, além de ser um espaço confiável para os alunos, de modo que se sintam protegidos e acolhidos (OLIVEIRA, 2015). Os professores devem lecionar as aulas de maneira didática e motivada, tornando-as mais dinâmicas, para assim possuir uma maior atenção dos alunos. É interessante frisar que dar sentido ao que o estudante está estudando é importante para que ele saiba que aquilo pode ser utilizado fora da sala de aula, mostrando que a matemática é bem ampla como ciência e disciplina.

Conforme definido na Lei de Diretrizes e Bases da Educação Nacional (LDB, Lei nº 9.394/1996), a Base deve nortear os currículos dos sistemas e redes de ensino das Unidades Federativas, como também as propostas pedagógicas de todas as escolas públicas e privadas de Educação Infantil, Ensino Fundamental e Ensino Médio, em todo o Brasil.

A Base Nacional Comum Curricular (BNCC) é um documento que regulamenta quais são as competências e habilidades que se espera que todos os estudantes desenvolvam ao longo da escolaridade básica. A base é orientada por princípios éticos, políticos e estéticos traçados pelas Diretrizes Curriculares Nacionais da Educação Básica e têm propósitos que direcionam a educação brasileira para a formação humana integral e para a construção de uma sociedade justa, democrática e inclusiva.

Levando-se em consideração os documentos oficiais, é possível observar que existem recomendações de alguns métodos para melhoria do ensino e da aprendizagem matemática. Segundo a BNCC (BRASIL, 2018), as orientações dadas aos professores remetem às estratégias de ensino respaldadas na resolução de problemas e sugerem que devem partir dos

conhecimentos prévios dos alunos e ajudá-los a ampliar e dar sentido matemático a estes conhecimentos. Uma das competências presentes na BNCC pressupõe habilidades que podem favorecer a interpretação e compreensão da realidade pelos estudantes, utilizando conceitos de diferentes campos da Matemática para fazer julgamentos bem fundamentados.

Na observação dos estudos na área da Educação Matemática, nota-se a importância de se ter um conhecimento amplo acerca do contexto em que o aluno está inserido, para facilitar o entendimento de como determinado assunto a ser ministrado pode se tornar interessante e aproximar o estudante da matemática. Segundo D' Ambrosio (1991, p. 1), "[...] há algo errado com a matemática que estamos ensinando. O conteúdo que tentamos passar adiante através dos sistemas escolares é obsoleto, desinteressante e inútil". Deste modo, falar sobre criptografia e códigos oferece uma diversidade maior no que diz respeito a abordar determinados assuntos matemáticos, além de aproximar o aluno de algo que se faz presente em seu cotidiano e em momentos históricos importantes, expondo aspectos onde a matemática é útil e necessária.

O ensino da criptografia em sala de aula, mais que uma ferramenta didática que serve para contextualizar e solidificar assuntos matemáticos, também fornece possibilidades de diferentes métodos em que uma informação secreta pode ser decifrada. Segundo Olgin e Groenwald (2011, p.2), a criptografia é um exemplo de tema que pode ser abordado no Currículo do Ensino Médio, pois permite desenvolver atividades didáticas utilizando padrões e regras de codificação e decodificação.

A criptografia é um assunto importante e que tem despertado o interessante no contexto atual, sendo utilizado bastante em sala de aula. Assim, "acredita-se que seu uso possa motivar os alunos e ajudar o professor a contornar dificuldades ao tentar estimular seus alunos no aprendizado e nos conceitos relacionados com o ensino da Matemática", (MACHADO, 1997, p. 95).

O uso de teoria dos números para o ensino básico pode ser introduzido através da criptografia RSA, utilizando conceitos e percepções prévias dos alunos, para ser acrescentado assim um novo conhecimento. O professor pode relacionar algo do cotidiano do aluno em que se possa utilizar congruência modular e, desta forma, o aluno conseguirá com mais facilidade entender o significado de se trabalhar com restos da divisão e o motivo de ser aplicado este conhecimento de teoria dos números a um método seguro e eficaz de criptografia.

2.2 Percurso Histórico

A criptografia tem sido importante desde a antiguidade e atualmente tem estado presente em nosso cotidiano, em senhas, compras pela internet, conversas em aplicativos, caixas

eletrônicos, entre outras ações que precisam ser mantidas em segredo. A palavra criptografia deriva do grego *Kryptós,* "escondido", e *gráphein*, "escrita". (FIGUEIREDO, 2012, p. 44). O tema relacionado a criptografia desperta curiosidade nos alunos, principalmente quando conseguem entender que a matemática está por trás de tudo isto, além de observar que conhecimentos matemáticos podem ser aplicados na prática em uma realidade não distante da qual eles estão habituados.

À medida em que foram sendo necessárias novas formas e métodos para se enviar uma mensagem ou informação em segurança, os princípios da criptografia foram construídos. Em determinadas ocasiões se fazia necessária a utilização de mensagens secretas: nas guerras, espionagem e outros. Desde a antiguidade, o ser humano possui a necessidade de se comunicar e, ao longo dos tempos, as formas de comunicação foram passando por mudanças de acordo com a evolução tecnológica na sociedade.

O objetivo destas mensagens secretas era que apenas o destinatário pudesse compreendê-las. "As primeiras escritas secretas são do século V a.C. e são encontradas nos nove livros *As Histórias*, de Heródoto, historiador grego. Consistiam, na verdade, em esteganografia", (GANASSOLI; SCHANKOSKI, 2015, p. 5). Esteganografia é uma comunicação secreta, na qual se esconde a existência da mensagem, que só é revelada ao destinatário final. A palavra deriva do grego *steganos*, que significa coberto, e *graphein*, que significa escrever.

> O termo esteganografia ficou conhecido em 1499 em um livro de 3 volumes do monge Johannes Trithemius, que aparentemente era sobre magia, espíritos, religião, porém, mais tarde, descobriu-se que o livro relatava sobre esteganografia e criptografia, detalhando vários métodos para enviar uma mensagem (GANASSOLI; SCHANKOSKI, 2015, p. 5).

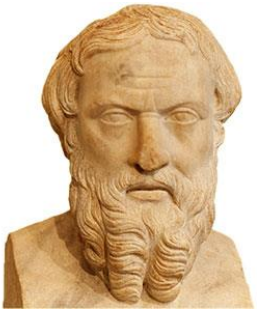
Situações como raspar o cabelo do mensageiro para tatuar uma mensagem secreta e aguardar o cabelo crescer, para assim enviá-lo ao destinatário que raspará novamente o cabelo do mensageiro para a mensagem ser lida é um exemplo. (GOMES, 2014, p. 19).

Os avanços da criptografia ao longo da história foram de grande importância para conseguir realizar o desejo de transmitir informações secretas de maneira eficaz. Serão destacados e apresentados alguns métodos acerca da esteganografia e criptografia, visando entender e compartilhar sua utilidade no decorrer dos anos.

Nascido no século V. a.C., Heródoto foi historiador, geógrafo e autor da história sobre a invasão Persa à Grécia, conhecida como *As histórias de Heródoto*. A obra, com suas histórias, informa que as mensagens enviadas aos gregos de como e quando Xerxes, o rei da Pérsia, iria atacá-los, eram escritas em pedaços de madeira e cobertas com cera. De acordo com Heródoto,

a Grécia foi salva da conquista por Xerxes graças a técnica da escrita secreta (SINGH, 2004, p. 5).

Figura 1 - Busto de Heródoto



Fonte: https://edukavita.blogspot.com/2015/06/biografia-de-herodoto-historiador-grego.html

Outro relato presente nessa obra é a história de Hiasteu, que raspou a cabeça para escrever instruções em segurança no seu couro cabeludo, com o cabelo crescido e a mensagem coberta, ela foi levada em segurança até a pessoa desejada, sendo revelada a mensagem raspando a cabeça novamente (SINGH, 2004, p. 6).

Após Heródoto, surgiram outras formas de esteganografia utilizadas na sociedade: por exemplo, no século XVI, um cientista italiano descreveu como esconder uma mensagem dentro de um ovo cozido escrevendo na casca com uma solução que só se torna visível quando se tira a casca. Algumas técnicas que eram capazes de esconder informações dentro de músicas, jornais e imagens também surgiram, mostrando que a esteganografia oferece alguma segurança, já que se manteve presente por um bom tempo, porém percebe-se a necessidade de uma cautela rigorosa para que esse método de enviar informações ocorra com sucesso.

Seria de grande importância algo que pudesse ultrapassar os limites da grande cautela necessária para se esconder uma mensagem, como na esteganografia. Desta forma, a criptografia surge com o intuito de esconder o significado da informação a ser transmitida e não esconder a mensagem em si.

O Bastão de Licurgo ou *scytale* (*σκυτάλη*, bastão em grego) ou cítala foi considerado o primeiro aparelho criptográfico utilizado pelos militares e criado no século V a.C. Apesar de alguns estudiosos inferirem que este tipo de cifra não passe de um mito, o bastão de licurgo é uma cifra de transposição, isto é, que se baseia apenas em rearranjar as letras de uma mensagem, de forma que as letras mantenham sua identidade, mas mudem de posição. Este método foi utilizado pelos soldados espartanos, que consistia em um bastão de madeira ao redor do qual se enrolava uma tira de couro longa e estreita. A tira deveria ser enrolada num bastão de largura igual ao qual a mensagem foi escrita e quando se tinha o bastão de mesma largura, a mensagem poderia ser revelada (OLIVEIRA, 2015, p. 15).

Figura 2 - Cítala

Fonte: https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-em-python/

Segundo Ganassoli e Schankoski (2015, p. 9) uma das primeiras apresentações da cifra por substituição aparece no texto Kamasutra, escrito no século IV a.C., que recomenda que as mulheres deveriam estudar 64 artes, entre elas, a *mlecchita-vikalpa* que é a arte da escrita secreta. Segundo Singh (2004, p. 26), a cifra de substituição é chamada desta maneira "...porque cada letra no texto é substituída por uma letra diferente, complementando assim a cifra de transposição."

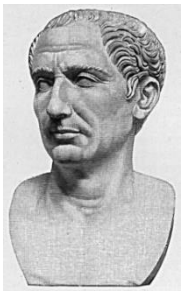
A criptografia por código é uma substituição de palavras ou frases por outras palavras, números ou símbolos. Deste modo, deve existir um dicionário para se codificar a mensagem, para que possa ser escrito o texto codificado e, quando chegar no destinatário, este deve possuir um dicionário semelhante para que a mensagem seja decodificada corretamente, como no exemplo a seguir:

Informação original	Informação codificada
PRAIA	UVA
BONITA	VERDE
Frase original	Frase codificada
PRAIA BONITA	UVA VERDE

Seria uma maneira mais segura de se criptografar, porém como cada destinatário deve possuir um dicionário chave, estas informações poderiam ser descobertas por pessoas que não foram escolhidas para receber determinado conteúdo, tornando fácil o acesso à decodificação quando se tem as informações necessárias.

A cifra de substituição foi utilizada para propósitos militares nas Guerras da Gália de Júlio César, que usava um cifrario para comunicar-se com as legiões romanas em combate pela Europa (GANASSOLI; SCHANKOSKI, 2015, p. 10).

Figura 3 – Busto de Júlio César



Fonte: https://pt.wikipedia.org/wiki/Cifra_de_C%C3%A9sar

A cifra de César funciona substituindo cada letra na mensagem por outra que está três casas à frente no alfabeto. Também é possível não deslocar três casas apenas, mas quatro, oito ou algum número entre as vinte e cinco casas, para fazer a substituição e obter mais 25 cifras de César diferentes.

Figura 4 - Código de César avançando 3 casas do alfabeto

Texto simples	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifra	D	E	F	G	H	I	J	K	L	M	N	O	P
Texto simples	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifra	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: https://recantododragao.com.br/2013/04/30/um-pouco-sobre-criptografia/

Caso fosse solicitada a codificação da palavra MATEMÁTICA, utilizando a tabela acima, teríamos PDWHPDWLFD, por exemplo. A chave é o que detalha como deve ocorrer a decodificação. Note que é imprescindível que o conhecimento desta chave seja apenas do receptor final, caso isto não aconteça, o inimigo conseguiria ler a mensagem facilmente.

Observe que códigos como estes são fáceis de quebrar, isto é, ler a mensagem mesmo não sendo o destinatário legítimo, o que acontece com códigos que substituem cada letra sistematicamente por outro símbolo qualquer. A razão para isto é o fato da frequência média em que cada letra aparece em um texto de determinado idioma ser constante. Na tabela abaixo, temos a frequência das letras no português: se for contabilizada a frequência de cada símbolo, é possível descobrir a que letra correspondem os símbolos mais frequentes.

Tabela 1 – Frequência das letras na língua portuguesa

Letra	**%**	**Letra**	**%**
A	14,64	N	5,05
B	1,04	O	10,73
C	3,88	P	2,52
D	4,10	Q	1,20
E	12,57	R	6,53
F	1,02	S	7,81
G	1,30	T	4,34
H	1,28	U	4,64
I	6,18	V	1,70
J	0,40	X	0,21
L	2,78	Z	0,47
M	4,78		

Fonte: Criptografia OBMEP , 2008

Em 1466, o disco de cifras, criado por Alberti, é o primeiro sistema polialfabético conhecido, sendo a primeira máquina de criptografia a ser criada. Consistia em dois discos que continham o alfabeto gravado e podiam ser girados: um deles continha o alfabeto original e o outro o alfabeto cifrado (OLIVEIRA, 2015, p.30). Segundo França (2014, p. 26), o disco de cifras é "um misturador que pega uma letra do texto normal e a transforma em outra letra no texto cifrado". Uma cifra que é monoalfabética usa apenas uma substituição fixa na mensagem inteira, enquanto uma cifra polialfabética utiliza mais que uma, o que proporciona um alto nível de dificuldade para desvendar o processo de decodificação, ocasionando numa segurança maior para as mensagens enviadas através da máquina de Alberti.

No final do século XVIII iniciou a Revolução Industrial, a qual proporcionou algumas mudanças culturais, sociais, políticas e econômicas. Suas principais características foram a grande expansão da produção, que deixou de ser baseada na manufatura, e a melhoria dos transportes (SENE MOREIRA, 2000). A Revolução Industrial ocasionou o desejo na sociedade da substituição do desgastante trabalho manual pelo mecânico e nada mais natural que a fase mecânica na criptografia também fosse alcançada: os primeiros indícios dessa nova fase para a criptografia ocorrem no início da idade moderna.

Figura 5 – Disco de cifras

Fonte: https://siriarah.wordpress.com/2014/04/23/criptografia-cifra-ou-disco-de-alberti-em-python/

Um engenheiro eletrotécnico alemão, chamado Arthur Scherbius, em 1918 patenteou uma máquina mecânica e elétrica com rotores, a qual é uma versão elétrica da máquina de Alberti. A máquina era chamada de Enigma e servia para criptografar e descriptografar as mensagens a serem enviadas (GANASSOLI, SCHANKOSKI 2015, p. 17).

Figura 6 – Arthur Scherbius

Fonte: https://pt.wikipedia.org/wiki/Arthur_Scherbius

Na criptografia mecânica é fundamental a ocultação pública da chave e também desejável manter segredo sobre a estrutura da máquina que produz a cifragem (FRANÇA, 2014, p. 25). A Enigma foi muito usada pelas forças militares alemãs, possuía três discos que eram os misturadores, as letras do texto original sofriam uma substituição através da rotação desses três discos, que continham as 26 letras do alfabeto, fornecendo assim, $26 \times 26 \times 26 = 17576$ ajustes diferentes de misturadores. Além disto, a máquina continha alguns plugues que ficavam na parte traseira que também fazia uma mistura, tornando bastante complexa e eficaz a mensagem codificada.

Figura 7 – Enigma

Fonte: https://blogs.ne10.uol.com.br/mundobit/2015/01/21/como-funcionava-enigma-maquina-nazista-que-quase-venceu-segunda-guerra/

Semelhante a máquina de escrever, pesava cerca de seis quilos e foi bastante útil, apesar de alguns matemáticos e equipes em países como a França, Polônia e Alemanha terem tido sucesso em quebrar o código da Enigma, foi preciso um processo complexo que decifrasse o modo como a máquina funcionava (SATURNINO, 2015).

As possibilidades numéricas da Enigma chegavam a cerca de seis sextilhões de códigos. Para a utilização da máquina, era preciso saber a posição inicial de uma sequência de três posições e existia um livro distribuído mensalmente pelos nazistas que informava quais rotores seriam utilizados, o que dificultaria bastante a descoberta da mensagem original.

2.3 A Criptografia RSA

Todos os métodos que apresentamos anteriormente envolvendo esteganografia e/ou criptografia conseguiram ser desvendados, alguns com um grau de dificuldade maior que outros. Porém, se fosse possível existir um processo que fosse fácil de codificar e muito difícil de decodificar, "ao utilizá-lo para criptografar uma mensagem, estaria garantido que quem a interceptasse, mesmo sabendo criptografar, teria um trabalho grande para decodificá-la" (COUTINHO, 2010, p. 7). Isso tornaria o processo de decodificação cansativo e a mensagem criptografada cada vez mais segura: o nível de dificuldade para desfazer o procedimento iria variar de acordo com os recursos disponíveis a quem interceptou a mensagem.

Os códigos destas mensagens são conhecidos como chave pública, pois a chave de codificação pode ser conhecida por qualquer um, sem comprometer a segurança do código. O problema matemático que satisfaz a condição que fornece a facilidade em codificar e a dificuldade em decodificar faz parte da área da matemática conhecida como teoria dos números, que estuda de modo geral as propriedades dos números inteiros.

Um dos métodos mais conhecidos de criptografia de chave pública é o RSA. Segundo Coutinho (2010, p. 9), "este código surgiu em 1977 por R. L. Rivest, A. Shamir e L. Adleman,

que trabalhavam no Massachussets Institute of Technology (M.I.T)", as letras RSA correspondem às iniciais dos inventores. Para utilizar este método, precisaremos fazer uso dos conhecimentos e técnicas da matemática presentes em teoria dos números.

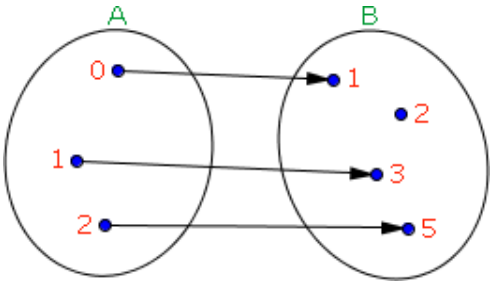
Suponha que será implementado o método RSA em uma loja de jogos, que será utilizado na codificação de dados de seus clientes nas compras feitas pela internet. Inicialmente seria preciso escolher dois números primos distintos e multiplicá-los, obtendo *n* um número inteiro, que será a chave conhecida. O que a loja deverá manter em segredo é a informação de quais foram os primos escolhidos, pois isso será necessário para decodificar as mensagens utilizando este método que está sendo implementado. Essa chave *n* será enviada para o computador ou celular de qualquer pessoa que compre na loja de jogos pela internet, pois é dessa chave que o computador do usuário irá necessitar para codificar os dados acerca do cartão de crédito e irá enviá-los para o computador da loja em questão, (COUTINHO, 2010).

De modo geral, o objetivo de obter um código que seja fácil de criptografar e difícil de descriptografar parte da multiplicação de dois números primos. Seria natural a ideia de, através da chave *n*, fatorar o número e encontrar os primos. No entanto, para números pequenos, encontrá-los seria algo trivial, porém estes números primos serão muito grandes. Na realidade, uma chave segura do método RSA é gerada a partir de números primos com cerca de 100 algarismos cada (COUTINHO, 2010, p. 18), de tal modo que a chave, que é o produto destes primos, possuirá cerca de 200 algarismos e quanto maior a chave *n*, mais tempo necessário para se fatorar um número grande e encontrar seus fatores primos. Além disto, podem ser necessários muitos anos para isto ocorrer em determinados casos, mesmo com toda a tecnologia existente atualmente.

Para realizar manualmente uma codificação através do método RSA é necessário ter conhecimento de três etapas: a primeira etapa é a pré-codificação da mensagem, a segunda etapa é a codificação da informação na qual será utilizada a chave de codificação *n*, e a terceira etapa é a de decodificação. Esta criptografia não seria eficaz se não possuísse uma maneira de descobrir o significado da mensagem codificada e pode-se perceber que o método só obtém sucesso caso corresponda a uma função bijetora, como mostraremos a seguir.

Suponhamos que o conjunto do lado esquerdo seja o conjunto de informações originais e o do lado direito o conjunto das informações codificadas. Note que no exemplo abaixo, existiria algo codificado que não corresponderia a nenhuma informação original, trazendo um problema para o método, visto que uma mensagem codificada não teria a representação de uma palavra, frase, texto ou símbolo, ou seja, não haveria significado para esta mensagem.

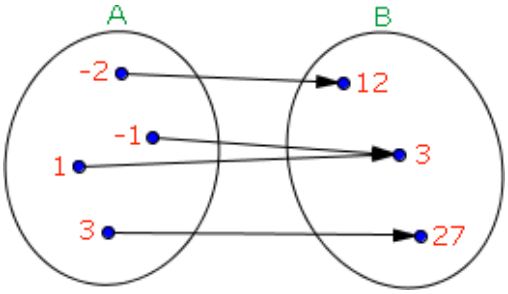
Figura 8 – Exemplo de função injetora



Fonte: http://www.matematicadidatica.com.br/FuncaoSobrejetoraInjetoraBijetora.aspx

Neste segundo caso, duas informações originais seriam levadas em uma mesma codificação. Quando fosse ocorrer a decodificação, ela poderia apresentar duas respostas diferentes, o que seria um problema, pois não se saberia qual das duas informações seria a correta.

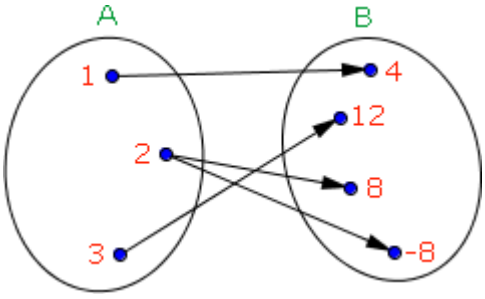
Figura 9 – Exemplo de função sobrejetora



Fonte: http://www.matematicadidatica.com.br/FuncaoSobrejetoraInjetoraBijetora.aspx

Perceba que se temos uma informação original e esta possui dois códigos diferentes, este método também não seria eficaz, pois se tenho duas representações para uma mesma mensagem, o destinatário estaria com um problema de ambiguidade e ocasionaria problemas na decodificação.

Figura 10 – Exemplo que não é função



Fonte: http://www.matematicadidatica.com.br/Funcao.aspx

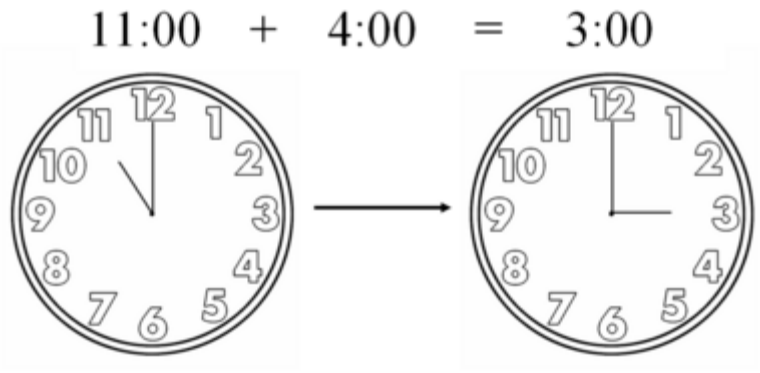
Portanto, para este método de codificação, a função que relaciona as informações desejadas pelo destinatário precisa ser bijetora.

A seguir, serão introduzidos alguns conhecimentos acerca de congruência modular com números inteiros, para assim dar início a execução da codificação através do método RSA.

Sabe-se que, durante o ensino básico, os alunos não estão acostumados a algumas notações e linguagens do conteúdo sobre teoria dos números. Então, ao se abordar criptografia, muitos deles provavelmente terão contato com o referente assunto pela primeira vez. Deste modo, transformar a linguagem densa em algo mais informal ajudará no processo de compreensão dos discentes. Antes de iniciar o assunto em si, o professor pode motivar o aluno questionando algo do cotidiano que tenha semelhança com a congruência modular, por exemplo, perguntar o caso em que a soma 11+4 = 3 seja verdade ou tenha algum sentido lógico. Após incitar a curiosidade, o professor pode relacionar a soma referida com o caso dos horários, isto é, 11+4= 15, quando se tem 15h no relógio, sabemos que é equivalente a informar que são 3h da tarde. A maioria dos alunos já ouviu falar que 14h se refere ao horário de 2h da tarde, que 20h se refere às 8h da noite, mas por qual o motivo isto acontece?

Observe que um relógio que é dividido em 12 partes: quando se inicia a contagem a partir do número um e chega ao número doze, o processo de contagem poderia continuar com 13, 14, 15 e assim por diante. Note que na figura abaixo quando somamos 11h mais 4h, temos que avançar quatro unidades no ponteiro referente às horas, então quando acrescenta-se quatro horas ao horário das 11h, tem-se que 11h+4h = 15h, mas quando é analisado o ponteiro das horas ele indica o número 3, ou seja, são 3h da tarde. Quando se diz que 15 horas possui uma associação para 3 horas da tarde, significa que esses números não são iguais, mas congruentes quando divididos por doze, que é o número de partes que o relógio está dividido.

Figura 11 – Congruência no relógio



Fonte: https://taylor.git-pages.mst.edu/index_files/Security/Content/04-AffineCipher.html

Como já foi comentado, será preciso ter conhecimento de algumas noções de teoria dos números para executar o método de codificação RSA. Diante disto, para facilitar o entendimento do processo serão apresentadas a seguir algumas definições, proposições e propriedades:

Definição 1.1 Se a e b são inteiros, dizemos que a divide b, denotado por $a \mid b$, se existir um inteiro c tal que $b = ac$. Se a não divide b escrevemos $a \nmid b$.

Exemplo 1.1

$5 \mid 15$, pois $15 = 5.3$

$4 \mid 12$, pois $12 = 4.3$

$2 \nmid 7$, pois $7 = 2.(3{,}5)$. Isto é, c não é inteiro.

Definição 1.2 Se a e b são inteiros, dizemos que a é congruente a b módulo m $(m > 0)$ se $m \mid (a - b)$. Denotamos isto por $a \equiv b (\mathrm{mod}\, m)$. Se $m \nmid (a - b)$ dizemos que a é incongruente a b e denotamos $a \not\equiv b \pmod{m}$

Exemplo 1.2

$7 \equiv 3 \pmod 4$, pois 4 | (7-3)

$17 \equiv 7 \pmod 5$, pois 5 | (17-7)

$27 \not\equiv 2 \pmod 4$, pois 4 $\nmid$ (27-2)

$19 \not\equiv 4 \pmod 2$, pois 2 $\nmid$ (19-4)

Deste modo, quando 21 horas se refere ao horário das 9 horas da noite, temos que $21 \equiv 9 \pmod{12}$, pois 12| (21-9).

Definição 1.3 Se a e b são dois inteiros com $a \equiv b \pmod m$, dizemos que b é um resíduo de a módulo m.

Exemplo 1.3: $9 = 2.4 + 1$, logo $9 - 1 = 2.4$. Pela definição de congruência, temos que $9 \equiv 1 \pmod 4$. Donde 1 é resíduo de 9 módulo 4.

A *divisão Euclidiana*, ou *divisão com resto*, é uma das quatro operações que as crianças aprendem na escola e é definida da seguinte forma:

Dados a e $b \in \mathrm{Z}$, com $b \neq 0$, existem q e $r \in \mathrm{Z}$ com

$$a = b.q + r \text{ e } 0 \leq r < |b|$$

Tais q e r estão unicamente determinados pelas duas condições acima e são chamados o $quociente$ e $resto$ da divisão de a por b. O resto r é também denotado por $a \bmod b$. Para o

exemplo da figura 11 isto significa que $11 + 4 = 15 \equiv 3 \pmod{12}$, isto é, a divisão de 15 por 12 deixa resto 3.

Proposição 1.1. Se a e b são inteiros, temos que $a \equiv b \pmod{m}$ se, e somente se, existir um inteiro k tal que $a = b + km$.

Demonstração: Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$, isto implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. Para a recíproca, suponhamos que existe k satisfazendo $a = b + km$, temos que $km = a - b$, donde $m \mid (a - b)$, isto é, $a \equiv b \pmod{m}$ o que conclui a prova. □

A congruência modular satisfaz algumas propriedades que a tornam muito semelhante à igualdade usual. A seguir, será provado que a congruência modular satisfaz propriedades análogas às da igualdade, mais precisamente:

Propriedade 1.1 Se a, b, c e m são inteiros, com $m > 0$, as seguintes sentenças são verdadeiras:

Reflexiva: todo número é congruente módulo m a si próprio; $a \equiv a \pmod{m}$

Simétrica: se $a \equiv b \pmod{m}$ então $b \equiv a \pmod{m}$;

Transitiva: se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$ então $a \equiv c \pmod{m}$;

Demonstração: Para mostrar que a congruência módulo m é reflexiva, verifiquemos que zero é múltiplo de qualquer número, logo temos que $m \mid 0$, então $m \mid (a - a)$, o que implica $a \equiv a \pmod{m}$. Passemos à simétrica: se $a \equiv b \pmod{m}$, então $a = b + km$ para algum inteiro k. Logo, $b = a + (-k)m$, o que implica $b \equiv a \pmod{m}$. Para a transitiva, se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem inteiros k e k' tais que $a - b = km$ e $b - c = k'm$. Somando-se membro a membro estas últimas equações, obtemos $a - c = (k + k')m$, o que implica $a \equiv c \pmod{m}$.

□

Até agora foram apresentados alguns resultados sobre congruências com números inteiros, neste momento será explicado como se calcula congruência modular com a presença de potências. Como dito ao longo do trabalho, congruência modular está associada com os

restos de uma divisão. Uma aplicação importante das congruências é o cálculo de restos de uma divisão de uma potência por um número qualquer.

Suponha que é desejado calcular o resto da divisão de 10^{135} por 7. Note que $10^6 \equiv 1 \pmod 7$. Dividindo 135 por 6 temos que $135 = 6.22 + 3$. Podemos através das propriedades de potências observar que $10^{135} = (10^6)^{22}.10^3$ e como $10^6 \equiv 1 \pmod 7$, podemos substituir 10^6 por 1 na congruência abaixo:

$$10^{135} \equiv (10^6)^{22}.10^3 \equiv (1)^{22}.10^3 \equiv 6 \pmod 7$$

Logo, $10^{135} \equiv 6 \pmod 7$. Como $0 \leq 6 < 7$ podemos concluir que o resto da divisão de 10^{135} por 7 é 6.

Exemplo 1.3: Qual é o resto da divisão de 2^{124512} por 31?

Se forem calculadas as potências de 2 módulo 31, pode-se observar que

$$2^2 \equiv 4 \pmod{31}$$

$$2^3 \equiv 8 \pmod{31}$$

$$2^4 \equiv 16 \pmod{31}$$

$$2^5 \equiv 32 \equiv 1 \pmod{31}$$

De modo parecido ao que aconteceu com as potências de 10 módulo 7, é possível descobrir uma potência de 2 que dá 1 módulo 31. Então desta vez, será usado $2^5 \equiv 1 \pmod{31}$ para fazer as simplificações. O expoente 124512 será dividido por 5 e vai ser obtido quociente 4016 e resto 2. Portanto,

$$2^{124512} \equiv 2^{24902 \,.\, 5+2} \equiv (2^5)^{24902}.2^2 \pmod{31}$$

Como $2^5 \equiv 1 \pmod{31}$, temos

$$2^{124512} \equiv (1)^{24902}.2^2 \equiv 4 \pmod{31}$$

Como $0 \leq 4 < 31$, podemos concluir que 2^{124512} deixa resto 4 na divisão por 31.

Retomando a criptografia RSA, para codificar uma mensagem utilizaremos uma tabela como auxílio do processo. Esta tabela irá representar as letras do alfabeto como números com dois algarismos, para não ocorrer ambiguidade. Esta escolha pode ser arbitrária e, neste caso, a

letra A foi representada pelo número dez e para as outras letras seguiu-se esta ideia consecutivamente.

Tabela 2 – Representação numérica das letras do alfabeto

A	10	N	23
B	11	O	24
C	12	P	25
D	13	Q	26
E	14	R	27
F	15	S	28
G	16	T	29
H	17	U	30
I	18	V	31
J	19	W	32
K	20	X	33
L	21	Y	34
M	22	Z	35

Fonte: Autora, 2020

A primeira etapa consiste em pré-codificar a mensagem desejada, que ocorre através da tabela 2. Veja um exemplo:

MENSAGEM	PRÉ-CODIFICAÇÃO
RSA	272810

Feita esta primeira parte, precisamos ter uma chave de codificação, que é o produto de dois primos, obtendo a chave *n*.

$$\mathbf{n} = p.q$$

Nesta chave *n*, p e q são números primos. Neste exemplo, tome p como sendo 5 e q como 7. Daí é obtida a chave será

$$\boldsymbol{n} = 5.7 = 35$$

Agora separe em blocos a pré-codificação da mensagem RSA. A separação será feita por dois algarismos, resultando em 27-28-10. Esta escolha também é aleatória. Esta pré-codificação pode ser separada em blocos de tamanhos diferentes, porém cada bloco não deve ultrapassar o número da chave de codificação, isto é, não poderá ter um bloco 36 neste exemplo, pois a chave é 35, logo não respeitaria a limitação desejada.

Cada bloco será codificado separadamente. Os blocos serão elevados a um mesmo número natural θ, para descobrir qual o resto da divisão desse número módulo 35, que é a chave n. Isto é, pretende-se saber qual a classe de equivalência desse bloco módulo n. De modo geral:

$$\text{Regra de codificação: } b^{\theta} \equiv a \pmod{n}$$

Feito isto, para exemplificar a utilização da regra acima, considere $\theta = 7$. O primeiro bloco a ser codificado será o 27, segue-se que:

$$27^7 \equiv (-8)^7 \equiv [(-8)^2]^3.(-8) \equiv 64^3.(-8) \equiv (-6)^3.(-8) \equiv 48 \equiv 13 \text{ (mod n)}$$

$$27^7 \equiv 13 \text{ (mod n)}$$

O bloco 27 foi codificado para o número 13. Após fazer o mesmo processo para os outros blocos, obtemos:

$$28^7 \equiv 7 \text{ (mod } 35)$$

$$10^7 \equiv 10 \text{ (mod } 35)$$

Os blocos 27-28-10 foram codificados para os blocos 13-7-10. Deste modo, a mensagem RSA foi codificada.

Para realizar o processo de decodificação de uma mensagem é essencial uma chave de decodificação que é formada por um par de números:

$$\text{Chave de decodificação } (n\,, d)$$

O número n já é conhecido do processo anterior e d corresponde a:

$$d = \text{inverso de } \theta \text{ [mod}(p-1).(q-1)]$$

Observe que para realizar a decodificação, precisaremos utilizar conhecimentos sobre a existência de inverso em teoria dos números. Para o leitor que desejar mais informações sobre a decodificação, veja o livro da OBMEP sobre criptografia (COUTINHO, 2010, p.79-97). Como o processo de decodificação não será foco da atividade aplicada aos alunos, não será abordada neste trabalho.

Há uma segurança neste método RSA, pois a decodificação depende do conhecimento dos primos p e q e, como visto anteriormente, a chave de codificação é conhecida, mas este número pode ser tão grande que fatorar para encontrar estes primos levaria muito tempo. Então o processo de codificação e decodificação do método RSA é simples e eficaz, transformando algo relativamente complexo em algo mais acessível.

3 RPG

Roleplaying Game ou RPG, que tem como significado na língua portuguesa "jogo de interpretação de papéis ou jogo de representação", teve sua primeira publicação no ano de 1973, nos Estados Unidos, sob o título DUNGEONS & DRAGONS, e tratava de fantasia medieval que tinha como fundamentação o universo e as aventuras da obra do escritor e professor de filologia de Oxford, J.R.R. Tolkien. Assim, desde a sua criação, o RPG se apresenta vinculado à literatura fantástica (VASQUES, 2008, p.12). É de modo geral um jogo de contar histórias, que são as aventuras. Cada partida é denominada sessão de jogo e quando uma aventura tem mais de uma sessão, esta é chamada de campanha. Em meio às diversas formas de se jogar *Roleplaying Game*, o RPG de mesa é o mais tradicional e possibilita o uso de menos recursos materiais para sua realização. A partida do RPG nessa modalidade se inicia através do narrador, que é denominado mestre do jogo e tem a responsabilidade de preparar com antecedência o esboço da aventura e zelar pela boa execução da mesma, apresentando seus desafios e surpresas a cada narração, para assim envolver mais ainda os jogadores participantes (TOLEDO, 2014, p.12). O restante dos jogadores fará a interpretação dos personagens principais da aventura do jogo e definirão suas falas e ações de acordo com a narração do mestre. Diante disso, é apresentada uma situação inicial, isto é, o mundo em que a aventura se encontra e quais os outros personagens envolvidos, que podem ou não ser interpretados pelo grupo, alguma informação extra que possa influenciar a aventura, sejam sobre lendas, fatos históricos, entre outros. Além disso, é descrito o cenário em que os personagens principais estão inseridos, para assim dar início a algum acontecimento em que os participantes enfrentem a aventura, que se dá geralmente a partir de uma situação-problema.

Os objetivos do jogo variam de acordo com a aventura escolhida e podem variar desde um tema medieval, à colonização de algum local não habitado ou guerras, por exemplo. A criatividade e as estratégias são muito importantes durante as partidas, inclusive do mestre, que utiliza sua imaginação para a criação das aventuras e inserção dos jogadores principais nessa história, que é produzida de forma coletiva (AMARAL, BASTOS, 2011, p. 4). Como podemos observar, o mestre tem que entender bem o universo fictício da aventura para assim ser o detentor de todas as chaves e segredos que envolvem o jogo. Ele também prepara as possibilidades que a história pode acarretar de acordo com as decisões dos participantes, sendo necessários improvisos e imaginação das possíveis ações a serem escolhidas pelo grupo para assim dar continuidade à aventura caso o grupo se direcione para alguma ação não planejada ou pensada pelo mestre, ou seja, o narrador constrói uma espécie de lista de possibilidades em que os jogadores estão constantemente interferindo.

É de responsabilidade dos jogadores interpretar os seus personagens de maneira eficaz, tomando as ações de acordo com o que foi informado pelo mestre. Assim, os jogadores irão falar qual a atitude que o personagem irá executar através da situação apresentada pelo mestre. No jogo de RPG, os personagens possuem dados com valores numéricos que são analisados como os atributos do personagem, isso serve para saber o sucesso ou fracasso de uma ação pretendida. Como há diversidade no RPG, cada sistema possui atributos que são próprios, mas é comum existir destreza, inteligência, vitalidade e força. A destreza equivale a uma medida da agilidade e da coordenação do personagem, a inteligência é relacionada à capacidade mental, a vitalidade está relacionada à saúde do personagem e a força, é uma força física do personagem.

O jogo também possui uma ficha de personagem, onde os valores desses atributos são escritos. Nesta ficha também pode conter outros dados com vantagens ou desvantagens, que podem ajudar o personagem ou prejudicá-lo ao longo da partida. O personagem, em determinadas situações durante a aventura, precisa testar os seus atributos, e para isso o jogador utiliza os dados para conferir o valor obtido com o escrito em sua ficha de seu personagem, esses valores diferem para cada sistema de regras. No livro *RPG nas escolas: Aventuras pedagógicas* (AMARAL, 2013), o autor apresenta uma sugestão para critérios numéricos em relação aos dados lançados, que será visto posteriormente.

O mestre também pode interpretar todos os demais personagens que possam aparecer ao longo da história. São os personagens coadjuvantes, que sempre fornecem informações providenciais aos jogadores no decorrer da aventura, e os antagonistas, que são os que oferecem obstáculos ou resistência ao grupo. São denominados na maioria das vezes por “Personagens do Mestre” (PdM) ou Non Player Caracteres (NPC, os personagens de nenhum jogador). (AMARAL, BASTOS, 2011, p. 5).

O RPG é um jogo de caráter coletivo e cooperativo já que o objetivo das aventuras envolve as ações de todos os personagens, em que os mesmos só atingirão o que se deseja quando se unem e trabalham em equipe para assim alcançar o sucesso durante a partida. Podemos perceber também que o RPG utiliza bastante a imaginação, fazendo com que o jogador se transporte para cenários e pensamentos diferentes quando provocados pelo mestre, isto é um ótimo motivo para observar o RPG como um material lúdico e uni-lo à educação. Segundo Pavão (2000, p. 5) um dos primeiros indícios do uso do RPG através das práticas pedagógicas foi por volta dos anos de 1990, pelo menos aqui no território brasileiro.

Figura 12: Exemplo de RPG

Fonte: http://basenacionalcomum.mec.gov.br/implementacao/praticas/caderno-de-praticas/ensino-fundamental-anos-finais/58-rpg-o-universo-da-imaginacao

3.1 Utilização do RPG em sala de aula

Quando o RPG está relacionado às disciplinas escolares se transforma em uma ferramenta interdisciplinar que, além de estimular a imaginação e criatividade dos jogadores, propõe a aplicação dos conhecimentos absorvidos na escola em situações do cotidiano.

> Entre aqueles que utilizam o RPG em sua sala de aula, há uma concordância de que o recurso impressiona pela capacidade de levar seus alunos a um nível de aprendizado diferenciado, pelo qual os estudantes demonstram o desejo em aprender mais sobre os conteúdos explorados. Talvez porque a aula se desenvolva de uma forma descontraída e prazerosa, em que todos têm o direito de falar e expressar opinião, ou porque os alunos consigam associar os conteúdos imediatamente a uma situação prática. No entanto, muitos professores não conseguem adotá-lo (AMARAL, 2013, p.7).

Rousseau defendia a utilização de atividades lúdicas para que as crianças conseguissem assimilar ações úteis, tentando vincular prazer e trabalho (DUFLO, 1999, p. 54). Na prática docente, sabe-se a existência do desinteresse presente em alguns alunos acerca de determinada matéria ou conteúdo. O professor pode utilizar o RPG como método de aprendizagem a fim de cativar e despertar um maior interesse pela disciplina e consequentemente um melhor desempenho do aluno. Além disso, o professor pode elaborar suas próprias aventuras para uma maior autonomia do que será utilizado, ou seja, com esta liberdade o professor pode criar uma aventura com o conteúdo que desejar, além de conhecer de perto o funcionamento do cenário, desafios e personagens que irão compor sua aventura.

É válido ressaltar que o RPG pedagógico, utilizado na educação, e o *Roleplaying Game* possuem similaridades e diferenças: a maioria dos RPGs comuns são baseados em combates imaginários entre os personagens dos jogadores e personagens do mestre, enquanto o RPG

pedagógico tem como prioridade a solução de situações-problema a partir do uso dos conceitos científicos ou apresenta cenários em que se possam fazer comparações com os conteúdos estudados, trazendo o aluno para uma aplicação do seu conhecimento através desta ferramenta (AMARAL, 2013, p.13). Existem mudanças nas regras também visto que o RPG é um jogo com muitos detalhes, então as regras para o utilizado em sala de aula são um pouco mais simples do que aquelas usadas no jogo comercial. Isto é um fator relevante, pois o professor geralmente possui pouco tempo em sala de aula, então as regras mais simples tornam o jogo mais ágil durante a aplicação.

3.2 Sugestões durante a aplicação do RPG em sala de aula

Numa sala de aula na educação básica dificilmente haverá poucos alunos, devido a este motivo o RPG pedagógico será composto por personagens que serão representados por grupos, isto é, a depender da quantidade de estudantes, é interessante que o professor divida a turma em cinco grupos, por exemplo, em que cada grupo será um personagem para iniciar a aventura. Cada grupo deve agir coletivamente para decidir a ação do personagem e os cinco grupos/personagens devem trabalhar em equipe para alcançar o objetivo da aventura. É interessante que todos os componentes possam participar do grupo que estiverem inseridos. A maneira com que os personagens serão divididos em sala de aula pode ocorrer através de sugestões e escolhas democráticas. É possível partir de ideias que possam construir grupos que optem por agir coletivamente como apenas um personagem, ou pode ser feita uma divisão em que cada grupo inicie a aventura com os integrantes da própria equipe representando um personagem por aluno como uma partida tradicional de RPG. Neste caso, cada grupo deverá ter um mestre, que pode ser um aluno de cada equipe designado para guiar a aventura, mas isto pode acarretar problemas nos casos em que alguma equipe tenha alunos com pouca prática ou contato com o RPG.

No caso em que cada grupo representar um personagem, o professor poderá acompanhar melhor o andamento das ações e ter uma percepção mais ampla durante a aplicação, visto que ter muitos grupos executando a mesma aventura com várias decisões distintas pode fazer o docente perder um pouco o controle do que acontece no momento.

Acerca da duração das aventuras, é recomendado que o professor realize a aplicação do jogo em um dia em que possua mais de uma aula, de preferência consecutivas, principalmente se ainda for instruir os alunos com as regras e explicações devidas. Assim o docente terá mais tempo para cumprir aquilo que deseja. Também é importante que o planejamento ultrapasse um pouco do tempo previsto para a finalização da aventura, pois sempre há oscilações com o que

se planeja e com o que acontece durante a prática, a depender do andamento e ações dos alunos ao longo da aventura.

No RPG existem dois tipos de personagens, aqueles que atuarão na história como personagens dos jogadores (PJ) e os personagens do mestre (PdM) que, sendo o criador da aventura, deve pensar nos coadjuvantes que irão compor a história, informando o que cada personagem terá de pontos característicos. Assim, no que diz respeito aos atributos do personagem, o criador pode pensar qual vitalidade (VT) que cada personagem terá, correspondente a uma medida da energia e da saúde, o que representa a quantidade de dano físico que o personagem é capaz de suportar antes de desmaiar ou morrer (AMARAL, 2013, p. 28). Além disso, é através do lançamento de dados que é verificado se o personagem consegue executar ou não determinada ação. Os dados podem variar de acordo com seu número de faces, o mais comum é o dado de 6 faces.

O livro *RPG nas escolas: Aventuras pedagógicas* (AMARAL 2013) sugere a seguinte relação:

Tabela 3: Quadro de sugestões para valores da vitalidade

VT	Descrição
6	O personagem corresponde a uma pessoa fraca, ferida ou com uma doença grave.
9	O personagem corresponde a uma pessoa comum, saudável e normal.
12	O personagem corresponde a uma pessoa acima da média (atleta, herói, etc.).

Fonte: AMARAL, 2013

As Habilidades (HB) estão relacionadas ao que o personagem sabe ou consegue realizar, tendo muitas opções para serem escolhidas, como adestramento de animais, arrombamento, escalada, fuga, pescaria e muitos outros. As habilidades podem ser apresentadas como abaixo:

Nome da habilidade
Descrição da habilidade

Exemplo: **Criptografia** − O participante consegue enviar mensagens em códigos criptografados de maneira que ninguém além do destinatário consiga decifrá-las, a não ser que o perseguidor da mensagem possua perícia em decifrar códigos e obtenha sucesso num teste de habilidade (AMARAL, 2013, p.32).

Normalmente, nem todas as pessoas que estudam algum assunto conseguem compreendê-lo na mesma intensidade, por isso cada habilidade que um personagem adquirir deve ser acompanhado de um número nomeado por Nível de Habilidade (NH), que informa o quão bem ele domina determinado assunto, que vai de 1 a 3 pontos. Para atribuir os níveis em

cada uma das habilidades escolhidas, você deve usar os pontos de sua VT (AMARAL, 2013, p.36). Ou seja;

Pontos de habilidades = VT

Tabela 4 – Relação com a habilidade ou os sentidos

NH	Relação com a habilidade ou sentidos
1	Aprendeu o mínimo necessário para fazer uso da habilidade./ Pode ouvir ou ver muito bem.
2	Sabe utilizar bem a habilidade, na maioria das vezes/ Pode ouvir ou ver melhor que a média.
3	É um especialista em relação à habilidade/ Pode ver coisas bem escondidas ou pequenas e ouvir pequenos ruídos e sons abafados.

Fonte: AMARAL, 2013

O nível de dificuldade (ND) representa o quão difícil é conseguir realizar uma determinada ação ou perícia. Estes níveis podem variar desde muito fácil até o quase impossível (AMARAL, 2013, p.39).

Tabela 5 – Sugestões para valores numéricos nos dados

ND	Ação	Exemplos
4	Muito fácil	Ouvir um barulho forte numa noite silenciosa, atravessar um rio calmo e raso, etc.
6	Fácil	Subir uma escada, ouvir pisadas furtivas num local silencioso, atravessar um rio calmo com água até o peito, etc.
8	Mediano	Subir numa árvore, ouvir pisadas furtivas num local silencioso, atravessar um rio calmo nadando, etc.
10	Difícil	Escalar um muro de pedras, ouvir pisadas furtivas num ambiente normal, atravessar um rio caudaloso nadando, etc.
12	Muito difícil	Escalar um paredão de rocha, ouvir pisadas furtivas enquanto está distraído, atravessar um rio caudaloso nadando carregando alguém, etc.
14	Quase impossível	Escalar um imenso bloco de gelo, ouvir pisadas furtivas num local barulhento, atravessar uma enxurrada nadando.

Fonte: AMARAL, 2013

Suponha, por exemplo, que a personagem Eva é uma especialista em pilotagem (o que lhe dá um nível na habilidade de 3 pontos). Para sobrevoar uma área com ND 10, Eva conseguiu tirar nos dados um 8. Daí: 8 + 3 = 11 > 10, então o personagem consegue sobrevoar a área. Se Eva tirasse o mesmo valor para sobrevoar uma área perigosa, com ND 14, ela possivelmente não conseguiria. Poderão existir outras características relacionadas aos personagens, como

defesa, ataque, riqueza de personagens e outros, que o professor poderá utilizar para encorpar sua aventura.

Para finalmente iniciar a aventura, o professor deve estar familiarizado com as regras que forem utilizadas e é interessante que, antes de iniciar a aplicação, sejam expostos aos alunos os objetivos desejados com o jogo e como isso o docente poderá auxiliá-los para uma melhor aprendizagem e integração entre a turma. Segundo a BNCC (2018, p. 99), uma das competências a serem desenvolvidas no ensino básico é de "utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e adequação das soluções propostas, de modo a construir argumentação consistente". Diante disto, o RPG pode ser uma ótima ferramenta para alcançar competências e habilidades previstas pela Base, inclusive com o assunto de criptografia, no sentido da criação de uma aventura em que os alunos possam utilizar os conhecimentos em relação à teoria dos números e conceitos de outros métodos de criptografia citados neste trabalho.

4 APLICAÇÃO E ANÁLISE

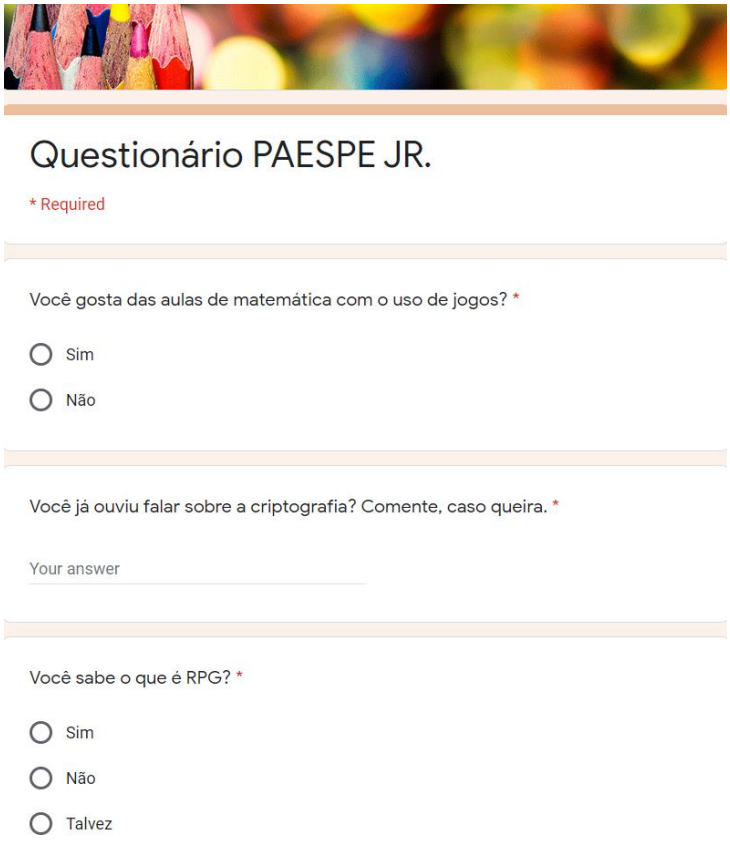
O público alvo da atividade planejada foram os alunos do Programa de Apoio aos Estudantes de Escola Pública do Estado (PAESPE) da Universidade Federal de Alagoas (UFAL). O PAESPE é uma iniciativa social que surgiu em 1993 coordenada pelo professor Roberaldo Carvalho de Souza, visando atender às necessidades da comunidade socialmente vulnerável, mais especificamente estudantes de escola públicas. Além disso, o PAESPE foi certificado pela Fundação do Banco do Brasil (FBB) como uma Tecnologia Social. Tal certificação é fruto das aulas ministradas pelos professores participantes do projeto, pois desenvolvem um trabalho humanizado em um contexto condizente com a realidade dos integrantes. "Considera-se tecnologia social todo o método, produto, processo ou técnica criado para solucionar algum tipo de problema social, atendendo os quesitos de simplicidade, baixo custo, fácil aplicabilidade e impacto social comprovado" (PAESPE, 2019).

O Programa PAESPE possui dois projetos, o PAESPE JR, que tem como público alvo estudantes da 2ª série do ensino médio, e o PAESPE, que se destina aos alunos que estão cursando a 3ª série do ensino médio. No PAESPE JR., projeto em que foi realizada a aplicação deste trabalho, são ministradas aulas de português e matemática, com o intuito de sanar as principais dúvidas dos conteúdos básicos escolares para assim fornecer melhor aprendizagem nos conteúdos futuros. No outro projeto, PAESPE, os alunos participam de aulas de todas as disciplinas escolares, visando principalmente à aprovação no Exame Nacional do Ensino Médio (Enem). O programa além de proporcionar aulas gratuitas também realiza visitas técnicas, tutoria, curso de informática básica, momentos com profissionais da psicologia e palestras, além de possuir uma infraestrutura com biblioteca e bom espaço para estudos. As provas de seleção são realizadas anualmente e os dois projetos juntos oferecem cerca de 200 vagas para estudantes da rede pública.

4.1 Aplicação da atividade

Para a aplicação deste trabalho, foi selecionada a turma do PAESPE JR que ingressou no fim do ano de 2019. Antes da aplicação, foi enviado um questionário online para a turma com três perguntas sobre criptografia, RPG e aulas com a utilização de jogos, a fim de diagnosticar o que maioria dos alunos conhece a respeito do conteúdo a ser ensinado. O questionário foi respondido por 69 de 80 alunos presentes nas duas turmas do projeto.

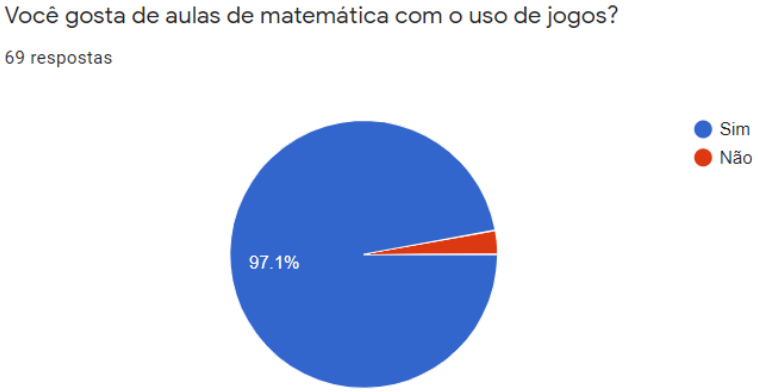
Figura 13 – Questionário online enviado antes da aplicação



Fonte: Autora, 2019

Os resultados do questionário seguem abaixo:

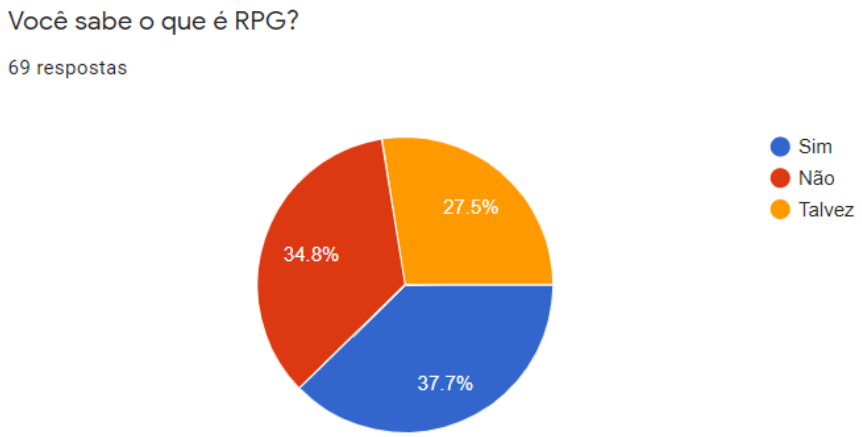
Figura 14 – pergunta sobre jogos do questionário online



Fonte: Autora, 2019

Na figura 14, sessenta e oito alunos afirmam gostar de aulas com o uso de jogos, expondo que na amostra apenas um aluno dentre os sessenta e nove não gosta de aulas com o auxílio de jogos durante a aula.

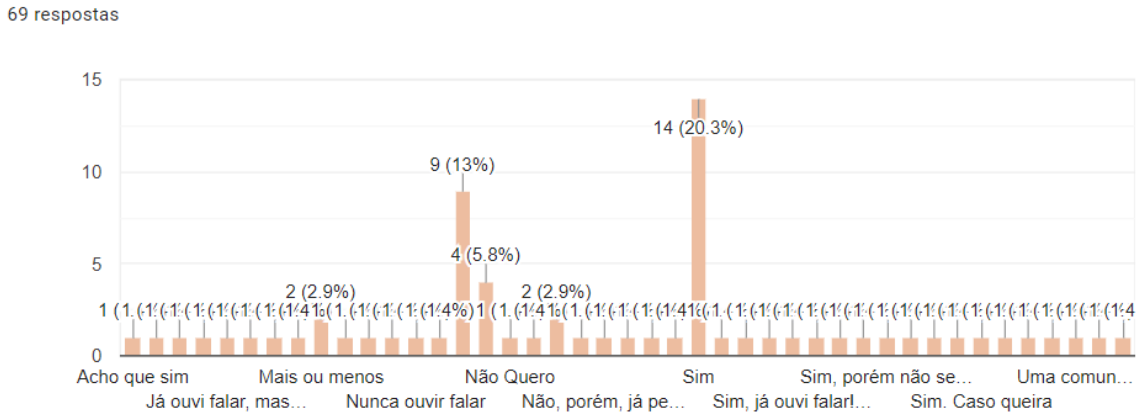
Figura 15 – pergunta sobre RPG do questionário online



Fonte: Autora, 2019

Na figura acima, não houve muita diferença quantitativa entre as respostas, mas de modo geral podemos inferir que a porcentagem de estudantes com dúvidas e desconhecimento sobre o RPG supera a porcentagem daqueles que conhecem.

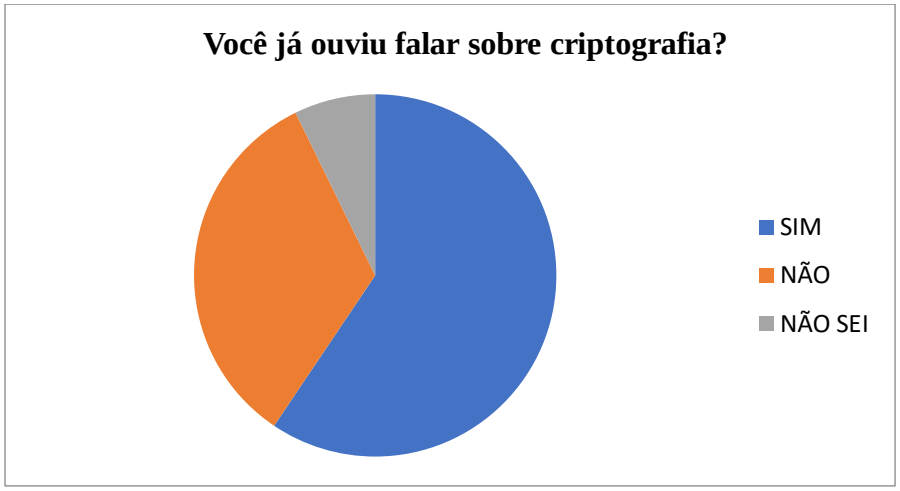
Figura 16 – Pergunta sobre criptografia



Fonte: Autora, 2019

A pergunta “Você já ouviu falar sobre criptografia?” deixava aberto para quem quisesse comentar algo a mais. Tabulando os dados de modo geral, 41 pessoas responderam que já ouviram falar sobre criptografia, 23 responderam que não sabiam ou nunca ouviram falar e 5 afirmaram não saber.

Figura 17 – Gráfico geral sobre a pergunta referente à figura 16



Fonte: Autora, 2019

É perceptível que maioria dos alunos já ouviu falar sobre o assunto de criptografia, porém não sabiam explicar bem o seu significado.

Como já dito, a aplicação da atividade, desenvolvida no projeto PAESPE JR., teve como proposta o ensino da criptografia aliada às noções de teoria dos números, juntamente com o uso do RPG para utilizar na prática o conteúdo aprendido. O planejamento inicial foi feito da seguinte forma: três professoras colaboradoras do programa incluindo a autora deste trabalho, sendo duas graduandas em matemática e uma graduanda em engenharia química. Estas seriam responsáveis pela aplicação nas duas turmas existentes. No primeiro momento, em uma turma, a autora deste trabalho ministraria a parte teórica sobre criptografia e na outra turma a aula seria exposta por uma professora voluntária do programa utilizando a sequência didática elaborada pela autora. Já no momento da aplicação do jogo, outra professora voluntária que já teve contato com o uso do RPG em sala de aula também iria auxiliar durante a execução da aventura em uma das turmas. A disponibilidade para a realização da atividade foi de quatro horas, para serem divididas entre aula e utilização do jogo. Nas duas primeiras horas o intuito foi de apresentar algumas formas de criptografia, inclusive a RSA, e explicar sobre o RPG, além de esclarecer como se joga no ambiente escolar. Os alunos possuem intervalo de 20 minutos, restando um total de 1h40min para a execução do jogo. Foram feitas pesquisas históricas, geográficas em revistas, livros e sites, para a criação da aventura com o intuito de melhor aproximar o tema abordado cujo foi sobre uma missão na guerra, relacionando fatos verídicos e fictícios, além dos problemas propostos e disciplinas envolvidas na aventura. Também foi prevista uma premiação final para todos os participantes, a entrega de materiais de auxílio para os alunos, uma caixinha de som para reproduzir determinados sons e ambientes presentes na aventura

fornecendo uma realidade extra durante o jogo. Para melhor apresentar o planejamento, o plano de aula e a aventura de RPG utilizada na aplicação estão no apêndice deste trabalho.

A aplicação da atividade proposta ocorreu inicialmente como prevista: no primeiro momento foram apresentadas através da aula as diversas formas de criptografia ao longo da história, inclusive a criptografia RSA, informando suas características e como se dá o seu processo manual utilizando teoria dos números, também foram feitos exemplos de cada tópico para fixar melhor o que foi dado, nesta etapa foram utilizados recursos de apresentação multimídia, quadro branco, pincéis e celular para exemplificar com alguns alunos a criptografia presente neste aparelho tão utilizado. Além disso, foi exposto um pouco sobre como se jogar o RPG, que novamente seria explicado no segundo momento. Durante a aula as duas turmas possuíam juntas 74 alunos, e os mesmos foram bastante participativos, alguns apresentaram dificuldades pontuais na compreensão do conteúdo que serão discutidas com mais profundidade durante a análise dos resultados.

4.2 Descrição da aplicação da atividade

Após a apresentação do assunto, chegou o momento do uso do RPG como ferramenta pedagógica: nesta fase os alunos das duas turmas foram unidos em apenas um local aberto com cadeiras e mesas suficiente para todos. A ideia de unir todos os estudantes ocorreu com a intenção de obter uma melhor percepção durante a aplicação e pela vantagem de se ter três professoras voluntárias, incluindo a autora deste trabalho, durante a aplicação do RPG pedagógico.

Os alunos foram divididos em oito grupos com até 10 alunos cada um. Cada grupo representou um personagem, isto é, a aventura de RPG contou com oito personagens principais. A fim de facilitar a visualização dos participantes, os alunos também estavam com *TNT tecido* amarrados no corpo ou representado no local de cada equipe. Os alunos que escolheram onde e como representariam as suas respectivas cores.

Figura 18 – Exemplo de marcação com TNT

Fonte: Autora, 2020

Após serem divididos, foi explicado detalhadamente como ocorreriam as regras do jogo e como eles deveriam reagir de acordo com a aventura. Foi informado também como funcionaria o uso dos dados e a importância de agir coletivamente para cumprir o objetivo da missão, além de informar que a imaginação e criatividade ajudariam muito ao longo da aventura.

Sobre o material utilizado na aventura, cada equipe possuía dois dados de seis faces, daí os níveis de dificuldade apresentados na *tabela 5* foram modificados quando o número a se atingir nos dados fosse muito alto. Outro material utilizado foi uma caixinha de som com o objetivo de reproduzir alguns momentos da história para elevar o nível da realidade do jogo. Cada personagem/equipe possuía papéis para rascunho, ficha de personagem e uma tabela da criptografia usada por Júlio César para utilizar como auxilio durante o jogo.

Figura 19 – Tabela impressa do código de césar

Fonte: Autora, 2020

Figura 20 – Ficha de personagem

Fonte: Autora, 2020

Depois de distribuídos os materiais necessários aos personagens e feita a explicação de como os alunos iriam agir durante o jogo, deu-se início à aventura proposta. A aventura teve como mestra a autora deste trabalho e o auxílio das duas professoras voluntárias que ficaram coordenando e instruindo as equipes quando preciso. A aventura se baseava em adaptações e veracidades da história em relação à segunda guerra mundial e os alunos foram informados acerca do contexto que estavam inseridos e sobre qual a missão que iriam executar.

Cada personagem representava um (a) soldado (a) e poderiam desenhar, caso quisessem o seu *avatar*, além de terem a liberdade de escolher os nomes fictícios e alguma habilidade plausível, sendo fornecido pelas professoras o restante das informações sobre a força, VT e outros. A maioria dos alunos teve um bom comportamento e interesse muito grande que perdurou até o fim do jogo, a empolgação dos estudantes foi um ponto importante durante a execução da aventura, bem como com a estruturação prévia dos organizadores para que o planejamento ocorresse como o esperado. A utilização da caixinha de som com mensagens prontas de personagens extras da aventura, juntamente com algumas trilhas sonoras ligadas ao contexto da história, também foi um ponto a se considerar, pois foi perceptível durante a aplicação que os alunos gostaram e após a mesma também existiram comentários sobre este fato.

Os alunos também exprimiram uma imaginação muito criativa ao executar as ações do jogo, tais como ações individuais do personagem ou das ações coletivas que envolviam todos os personagens. Um relato surpreso antes da aventura foi o de uma aluna que no fim da aula teórica comentou que não gostava do RPG em si, pois havia participado de uma aventura em outra eventualidade e não achou interessante, daí após a experiência do RPG pedagógico a

mesma comentou que havia gostado de como ocorreu a aventura e que conseguiu participar, mesmo no início estando receosa pela opinião inicial de não gostar do RPG.

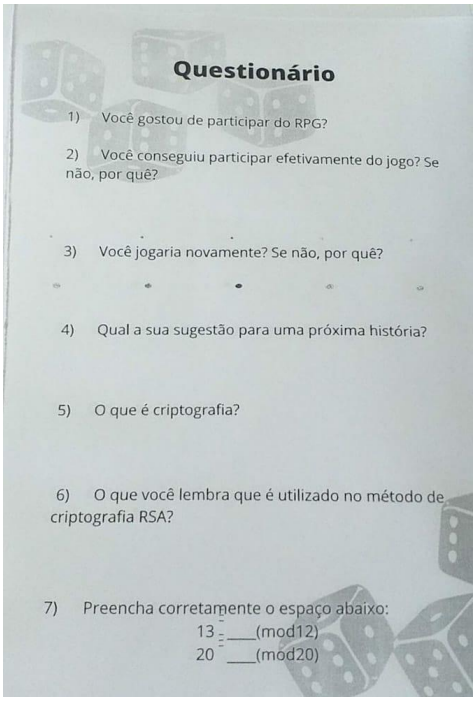
Os desafios presentes na história do RPG foram criados pensando em unir a aula teórica sobre o percurso histórico da criptografia, incluindo a RSA, e alguns assuntos de matemática básica que os alunos já haviam estudado anteriormente no PAESPE JR. Nos momentos da mestra narrar os acontecimentos e situações da aventura, os participantes se mantiveram atentos e precisavam estar mais quietos, para não existir dispersão e conversas paralelas devido à grande quantidade de alunos, já nos momentos de execução de ação ou de planejamento da mesma, os alunos eram livres para interagir, discutir e dialogar com os demais colegas. Os alunos também perceberam que para avançar na aventura e alcançar o objetivo final deveriam se esforçar para resolver os desafios, pois se um personagem viesse a desistir poderia comprometer toda a missão e com isso os alunos persistiram para solucionar os problemas propostos, conseguindo assim prosseguir no jogo.

Posteriormente será exposta a relação do referencial teórico com o envolvimento e comportamento dos alunos durante a aplicação, observando os questionários e os desafios presentes na aventura do RPG.

4.3 Análise dos resultados

Após o fim da aventura do RPG pedagógico, foram distribuídos questionários com sete perguntas. Sendo quatro questões sobre o jogo e satisfação de participação, e as outras três sobre criptografia e congruência modular. Na aplicação do questionário foram obtidas 71 respostas, dos 74 participantes (nem todos os alunos puderam responder, pois só havia 71 questionários impressos). Um dos pontos mais buscados ao longo do jogo foi o da participação de pelos menos maioria dos alunos, sendo constantemente observados e indagados sobre o que estava acontecendo, com o intuito de evitar que ficassem dispersos ou de apenas um aluno responder pelo grupo em todas as ações, fazendo com que outros estudantes não participassem efetivamente.

Figura 21 – Questionário pós-aplicação do RPG



Questionário

1) Você gostou de participar do RPG?

2) Você conseguiu participar efetivamente do jogo? Se não, por quê?

3) Você jogaria novamente? Se não, por quê?

4) Qual a sua sugestão para uma próxima história?

5) O que é criptografia?

6) O que você lembra que é utilizado no método de criptografia RSA?

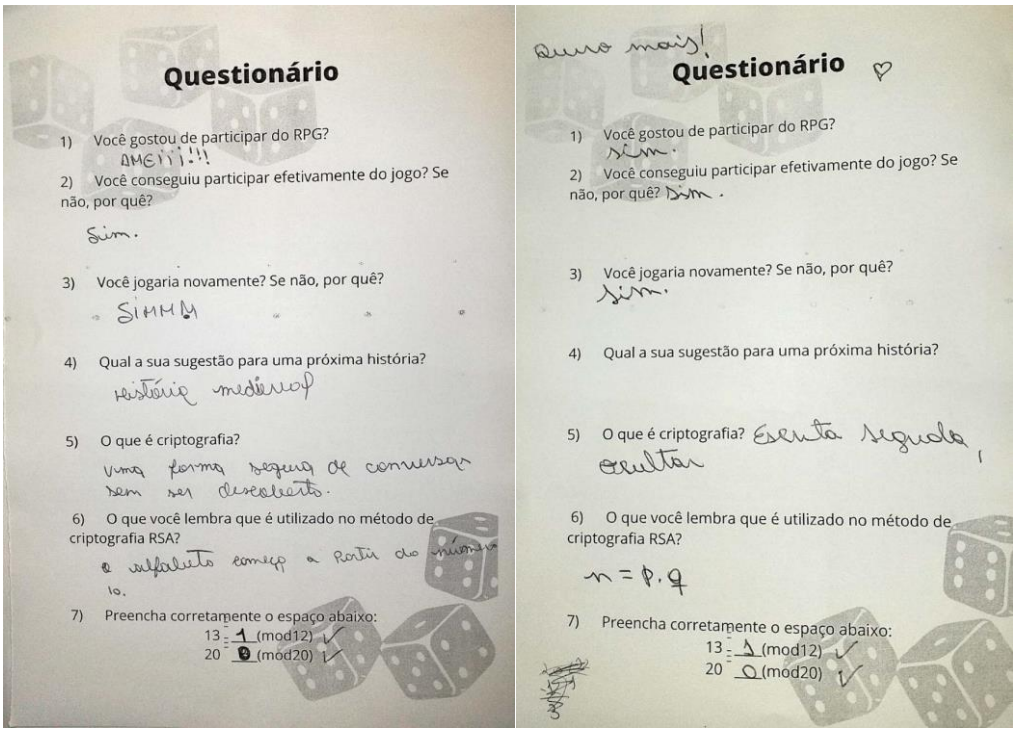
7) Preencha corretamente o espaço abaixo:

13 ≡ ___(mod12)

20 ___(mod20)

Fonte: Autora, 2020

Figura 22- Questionários respondidos por dois estudantes



Questionário

1) Você gostou de participar do RPG?
AMEIIII!!!

2) Você conseguiu participar efetivamente do jogo? Se não, por quê?
Sim.

3) Você jogaria novamente? Se não, por quê?
SIMMM

4) Qual a sua sugestão para uma próxima história?
história medieval

5) O que é criptografia?
uma forma segura de conversar sem ser descoberto.

6) O que você lembra que é utilizado no método de criptografia RSA?
o professor começa a partir dos números.

7) Preencha corretamente o espaço abaixo:
13 ≡ 1 (mod12) ✓
20 0 (mod20) ✓

Quero mais!

Questionário ♡

1) Você gostou de participar do RPG?
sim.

2) Você conseguiu participar efetivamente do jogo? Se não, por quê? sim.

3) Você jogaria novamente? Se não, por quê?
sim.

4) Qual a sua sugestão para uma próxima história?

5) O que é criptografia? Escrita segreda, oculta

6) O que você lembra que é utilizado no método de criptografia RSA?
$n = p \cdot q$

7) Preencha corretamente o espaço abaixo:
13 ≡ 1 (mod12) ✓
20 0 (mod20) ✓

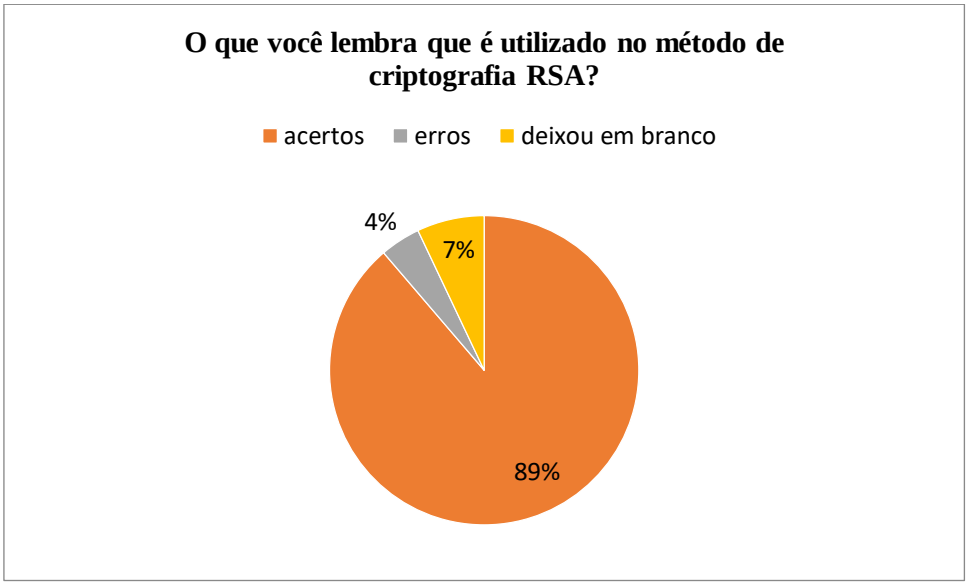
Fonte: Autora, 2020

Na pergunta cinco do questionário final da figura 21, todos os alunos responderam em uma linha de raciocínio coerente com o significado de criptografia apresentado durante a aula teórica.

Durante a aventura essas respostas foram comprovadas, pois quando os estudantes eram questionados sobre algo envolvendo a criptografia, os mesmos comentavam entre si seus significados, para ver se os auxiliavam durante os desafios da aventura, além de estarem bastante empolgados ao relembrar o conteúdo teórico, a fim de conseguir superar o desafio do RPG e prosseguir no jogo. Confirmando o que foi dito por Machado (1997, p. 95), a criptografia é um assunto importante e que tem despertado interesse no contexto atual, a fim de despertar um algo a mais nos alunos, os motivando e auxiliando o professor a contornar as dificuldades ao tentar estimular os alunos nos conceitos relacionados ao ensino da matemática.

Quando os alunos responderam a pergunta acerca da criptografia RSA, 89% acertaram a resposta, 7% deixaram em branco e 4% não responderam a pergunta corretamente.

Figura 23 – Resultados sobre a criptografia RSA



Fonte: Autora, 2020

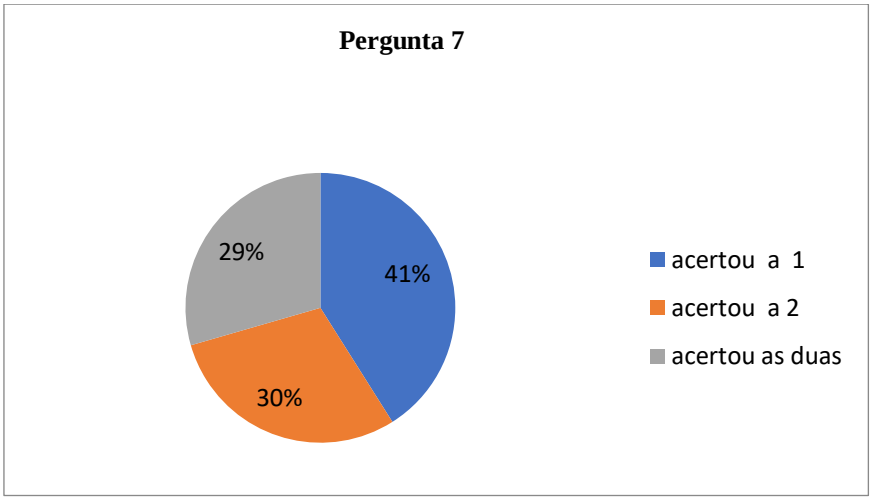
No questionário final, também foi colocada uma pergunta sobre congruência modular para analisar se os alunos haviam compreendido algo neste quesito. A pergunta solicitou que os alunos preenchessem o espaço corretamente das seguintes congruências:

$$13 \equiv \_ \ (mod\ 12)$$ **(1)**

$$20 \equiv \_ \ (mod\ 20)$$ **(2)**

Foi observado que 71% dos alunos acertaram pelo menos uma das duas congruências acima, 41% preencheram corretamente a primeira, 30% a segunda e 29% dos estudantes conseguiram preencher as duas lacunas de maneira correta como mostra a figura 28.

Figura 24 – Resultados acerca da congruência modular



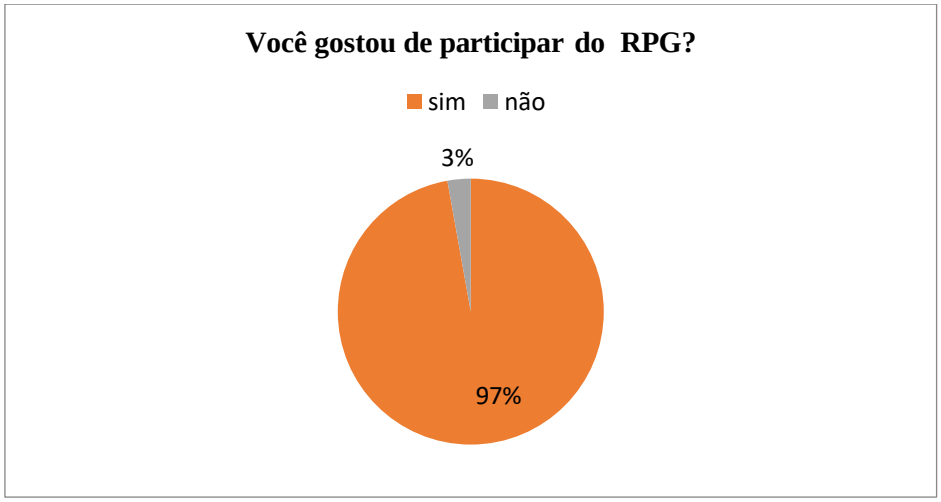
Fonte: Autora, 2020

O fato de se ter mais resultados positivos para a congruência um dá-se pela congruência modular presente nos relógios, visto que muitos alunos fixaram a ideia apresentada na figura 11. Por outro lado, não foram obtidos resultados em que algum aluno tenha errado as duas congruências, informando que pelo menos nesta análise quantitativa os estudantes estavam com alguma compreensão absorvida sobre o conteúdo de congruência modular.

Sobre a pergunta a respeito da satisfação por ter participado do RPG, foram obtidas sessenta e nove respostas para “sim” e duas respostas para “não”, como se pode visualizar na figura apresentada posteriormente. A satisfação dos alunos foi quase unanimidade e durante a aplicação foi perceptível a motivação deles durante a aventura, validando os pensamentos de Olgin e Groenwald (2011) que falam sobre o conteúdo de criptografia para desenvolver atividades didáticas.

No trabalho de Duflo (1999, p. 54), é constatado que Rousseau defendia a utilização de atividades lúdicas para que as crianças conseguissem assimilar ações úteis com o intuito de unir prazer e trabalho e, além disso, os estudos de Amaral (2013) relatam que quando o RPG está relacionado às disciplinas escolares se transforma em uma ferramenta pedagógica que além de motivar, estimulam a imaginação e criatividade dos participantes.

Figura 25 – Resultados sobre a satisfação de participação



Fonte: Autora, 2020

Na pergunta quatro da figura 21 foram recolhidas diversas ideias para uma próxima história/aventura de RPG. Os alunos expuseram sugestões envolvendo conteúdos políticos, históricos, culturais e comentaram que gostariam que a aventura tivesse uma duração maior. Com os relatos pós-aula e os expostos no questionário, podemos observar que a crítica de D'ambrosio (1991, p.1) sobre a matemática que está sendo ensinada pelos professores com métodos obsoletos e desinteressantes pode ser contrastada com a aplicação do RPG unida ao ensino de criptografia, pois o assunto de criptografia é atual e presente no cotidiano dos alunos e o RPG é um jogo que propõe algo diferente e interessante para maior parte dos participantes.

Ao fim da aula teórica três estudantes buscaram mais informações sobre os diversos métodos de criptografia e ainda falaram sobre métodos que eles conheciam, mas que não foram apresentados na aula. Juntando as participações em sala de aula com este relato, podemos dizer que os alunos ficaram motivados ao entrar em contato com o assunto ministrado. Isto revela que atividades diferenciadas em sala de aula, como o uso do RPG, resultam em consequências positivas, pois os alunos tendem a ter mais atenção e ainda são estimuladas a oralidade e coerência dissertativa, pois é um jogo que se vivencia pela fala (PAVÃO, 2000, p.3).

As figuras 26 e 27 a seguir mostram se os alunos conseguiram participar efetivamente do jogo e se os alunos jogariam novamente o RPG, respectivamente.

Figura 26 – Resultados sobre a participação efetiva

Fonte: Autora, 2020

Figura 27 – questionamento se os alunos jogariam novamente o RPG

Fonte: Autora, 2020

Apesar de terem alunos que afirmaram não ter participado efetivamente, um número grande informou que conseguiram agir coletivamente e informar suas opiniões ao grupo. Mas o professor deve ficar atento, para buscar incluir o maior número de pessoas possível durante a execução do jogo, um número menor de alunos talvez seja mais fácil de conseguir uma efetividade unânime.

Também existiu o caso de alunos terem participado efetivamente, mas que não jogariam novamente ou não sabiam se participariam, porém é preciso levar em consideração o aluno que desde o questionário diagnóstico afirmou não gostar de aula com o uso de jogos e daqueles que não gostam do RPG ou do tema abordado em si.

5 CONSIDERAÇÕES FINAIS

O sistema de educação no Brasil ao longo do tempo vem se modificando, desde o modo totalmente hierárquico da relação professor-aluno até as metodologias de ensino que vem tendo renovações e visões para melhor ajudar e compreender o aluno em seu processo de aprendizagem. Deste modo, é relevante que o professor busque inovações e métodos práticos de aulas mais atraentes para os estudantes que em sua grande parte acreditam em uma matemática sem sentido e sem aplicação em seu cotidiano.

Neste sentido, este trabalho apresentou uma ferramenta diferenciada através do uso do RPG pedagógico abordando tópicos de teoria dos números relacionados à criptografia para professores da educação básica, com o intuito de uma aprendizagem e participação efetiva de maioria dos participantes.

A aplicação executada neste trabalho pode ser praticada e adaptada para o público discente a partir do 9º ano, pois os alunos já terão tido contato com as operações básicas, potências e conseguem analisar com mais facilidade os restos de divisão, mas o professor que saberá o nível que deverá ser abordado dependendo da série ou ano que o aluno estiver cursando. O professor pode criar a própria aventura, podendo perguntar qual tema os estudantes tem um entusiasmo maior com a finalidade de adaptar a história ao que os alunos se sentem mais motivados.

Um fator interessante é que o RPG torna a aula interdisciplinar e mais animada, fazendo com que o professor tenha uma motivação maior e busque investir mais tempo para atividades diferentes nas escolas além das aulas tradicionais que são conhecidas. Neste trabalho também foi comprovado que os alunos têm um maior envolvimento na aula quando se deparam com desafios para além do lápis e papel, isto é, quando os mesmos conseguem relacionar o assunto com o cotidiano e assimilar a matemática com sua importância na sociedade.

Através da aplicação presente neste trabalho foram desenvolvidas algumas competências e habilidades previstas pela BNCC e existiram pontos positivos em relação ao modo com que o conteúdo foi introduzido aos discentes. Vale ressaltar que a aplicação do RPG pedagógico exige planejamento do professor e um bom conhecimento da aventura para que o jogo seja executado de modo eficaz, trazendo aprendizados e experiências sobre o que melhorar ou mudar em uma próxima aplicação.

O uso do RPG em sala de aula como instrumento para fixar o conteúdo foi uma experiência prazerosa como professora e diante dos resultados aqui expostos, para os estudantes também. Além do que foi executado nesse trabalho, o docente pode reinventar e realizar a

aplicação aqui lançada em diversas ocasiões escolares, como em oficinas, feira de ciências sobre a disciplina de matemática e outros que vão além da sala de aula.

Por fim, basta salientar que cada professor tem um papel de extrema importância na vida dos alunos que ele tem contato ao longo de sua carreira, podendo compartilhar conhecimentos, valores e sendo muitas vezes referência para alguns. A educação brasileira ainda precisa de muita transformação, porém o professor pode impactar vidas e transformá-las através do conhecimento com suas atitudes, métodos de ensino e empatia. Para gerar a mudança que queremos é necessário tomar atitudes e assim proporcionar qualidade de ensino e aprendizagem no ambiente em que nós professores exercemos o nosso papel.

6 REFERÊNCIAS

AMARAL, R. R., BASTOS, H. F., **O Roleplaying Game na sala de aula: uma maneira de desenvolver atividades diferentes simultaneamente**. Revista Brasileira de Pesquisa em Educação em Ciências, 2011.

AMARAL, R. **RPG na escola**: aventuras pedagógicas. Recife: Editora Universitária da UFPE, 2013.

BRASIL. **Base Nacional Comum Curricular: Ensino Médio**. Brasília: MEC/Secretaria de Educação Básica, 2018.

BRASIL. **Lei de diretrizes e bases da educação nacional**. Conselho de Reitores das Universidades Brasileiras, 1997.

CERQUEIRA, M. C., **O estudo da criptografia RSA no Ensino Básico com auxílio de softwares computacionais**. Maceió, 2016.

COUTINHO, S. C. **Criptografia.** Rio de Janeiro: IMPA/OBMEP, 2010.

D'AMBRÓSIO, U. **Matemática, ensino e educação:** uma proposta global. Temas & Debates, São Paulo, 1991.

DANTAS, A. A., **A criptografia no ensino fundamental e médio**. Caicó, 2016.

DUFLO, C. **O jogo:** de Pascal a Schiller. Porto Alegre: Artes Médicas Sul, 1999.

FIGUEIREIDO, L. M., **Introdução à criptografia**. Rio de Janeiro: Fundação CECIERJ, 2012.

FRANÇA, W. B. A. **A Utilização da Criptografia para uma Aprendizagem Contextualizada e Significativa**. Dissertação (Mestrado Profissional em Matemática) – Universidade de Brasília, Brasília, 2014.

GANASSOLI, A. P.; SCHANKOSKI, F. R., **Criptografia e Matemática**. Curitiba, 2015.

GOMES, Francisco Claudio Lima. **Uma proposta de abordagem no Ensino Médio da Criptografia RSA e sua estrutura matemática**. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal do Tocantins, Tocantins,2014.

MACHADO, N. J. **Matemática e realidade**. 4.d. São Paulo, Brasil: Cortez, 1997.

MALAGUTTI, P. L. **Atividades de contagem a partir da criptografia**. Rio de Janeiro, 2015.

OLGIN, Clarissa de Assis e GROENWALD, Cláudia Lisete Oliveira. Criptografia e o currículo de matemática no ensino médio. **Revista de Educação Matemática** – vol 13, número 15, 2011.

OLIVEIRA, G. R., **Algumas aplicações da criptografia no ensino fundamental**. Dissertação (Mestrado Profissional em Matemática) - Universidade Federal do Tocantins, Tocantins, 2015.

PAESPE, 2020. Disponível em: <http://www.ufal.edu.br/unidadeacademica/ctec/extensao/paespe>. Acesso em: 30 de abril de 2020.

PAVÃO, Andréa. **A aventura da leitura e da escrita entre mestres de Roleplaying Game**. 2. ed. São Paulo: Devir, 2000.

SATURNINO, L., Como funcionava a enigma, a máquina nazista que venceu a segunda guerra. Ciência, 2015.

SENE, Eustáquio; MOREIRA, João Carlos. **Geografia geral e do Brasil: espaço e globalização**. São Paulo: Scipione, 2000.

SINGH, Simon. **O livro dos códigos**. Editora Record, 2004. Disponível em: <https://pdfslide.net/documents/primeiro-capitulo-o-livro-dos-codigos-simon-singh.html>. Acesso em: 30 de abril de 2020.

TOLEDO, E. A., **RPG como estratégia de ensino**. Paraná, 2014.

VASQUES, R. C. **As potencialidades do RPG na educação escolar**. São Paulo, 2008.

WERNECK, H. **Ensinamos demais, aprendemos de menos**. 22 ed. Petrópolis: RJ, Editora Vozes, 2011.

7 APÊNDICES

APÊNDICE A

Disciplina: Matemática
Ano: 2ª série (Ensino Médio)
Conteúdo: Criptografia RSA, e as criptografias ao longo do desenvolvimento da sociedade.
Tempo estimado: 04 horas/aula
Prof (a): Ewellyn Amâncio Araújo Barbosa

PLANO DE AULA

JUSTIFICATIVA

O estudo da Criptografia é importante, pois possibilita ao aluno estabelecer conexões entre o conteúdo e o mundo. Além de utilizar conhecimentos anteriores de seu cotidiano para assimilar com as novas informações.

OBJETIVO GERAL

Apresentar o conteúdo de criptografia, além de utilizar noções de teoria dos números no tópico de criptografia RSA para posteriormente utilizar através do RPG pedagógico.

OBJETIVOS ESPECÍFICOS

- Ter conhecimento da definição de criptografia e suas características.
- Saber aplicar os conhecimentos de criptografia, seja em situações problema ou em exercícios com aplicação.

COMPETÊNCIAS E HABILIDADES (SEGUNDO A BNCC)

Competência específica (1): Utilizar estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos, sejam atividades cotidianas, sejam fatos das Ciências da Natureza e Humanas, das questões socioeconômicas ou tecnológicas, divulgados por diferentes meios, de modo a contribuir para uma formação geral.

Habilidades:

(EM13MAT106) Identificar situações da vida cotidiana nas quais seja necessário fazer escolhas levando-se em conta os riscos probabilísticos (usar este ou aquele método contraceptivo, optar por um tratamento médico em detrimento de outro etc.)

METODOLOGIA

Inicialmente serão levantados questionamentos sobre o assunto, já que se trata de algo presente no cotidiano e em várias formas de tecnologia. Após esse primeiro momento serão apresentados alguns métodos de criptografia e no método RSA serão apresentados algumas

	ideias e noções sobre teoria dos números informando sua utilidade para criptografar e descriptografar determinada informação.
RECURSOS DIDÁTICOS	• Quadro branco; • Pincéis para quadro branco; • Equipamento para Data Show; • Apresentação em Power Point; • Material ilustrativo; • RPG pedagógico
INTERDISCIPLINARIDADE	A interdisciplinaridade ocorrerá com as disciplinas de geografia e história.
CONTEXTUALIZAÇÃO	O conteúdo será contextualizado através das situações-problema do cotidiano que envolvam criptografia.
TEMAS TRANVERSAIS	Trabalho coletivo, ética, sociedade.
AVALIAÇÃO	A avaliação será de caráter formativo e contínuo, isto é, serão consideradas a participação e interações em sala de aula, as anotações feitas ao longo das explicações e a resolução dos exercícios propostos.
REFERÊNCIAS	http://basenacionalcomum.mec.gov.br/images/historico/bncc_ensinomedio_embaixa_site_110518.pdf

APÊNDICE B

AVENTURA RPG

AQUELE EM QUE OS SOLDADOS SE FERIRAM

O ano é 1939, os alemães acabaram de invadir a Polônia e a segunda guerra mundial se iniciou quando a França e a Inglaterra declararam guerra à Alemanha Nazista. Após alguns anos de conflito, duas forças se formaram, os Aliados são compostos por: Inglaterra, França, Estados Unidos e União Soviética e o Eixo é composto por: Alemanha, Japão e Itália.

Cena 1: A Missão Suicida (descrição e distribuição das fichas)

Um pelotão do exército francês foi levado em cativeiro durante uma batalha de Dunquerque e informações importantes de guerra podem vazar através da tortura imposta sobre os franceses. Por isso, vocês, um grupo de soldados e soldadas de elite do lado das forças Aliadas têm a missão de resgatar os franceses e restabelecer o equilíbrio do combate. A ação deve ser furtiva, silenciosa e ágil, pois as forças inimigas têm um número elevado de soldados na base onde estão os reféns.

Desafio 1: Salto de paraquedas

Vocês deverão partir ao entardecer num avião de espionagem, o avião não pousará no território inimigo para não ser detectado, por isso vocês devem saltar de paraquedas a uma altitude de 13 mil pés. O nível de dificuldade para o salto é mediano, pois o avião está em movimento. Sabendo que um salto demora, em média, 7 minutos no total (a partir do momento da largada do avião até o solo), e que o tempo que o paraquedista deve passar com o paraquedas aberto é de 6 minutos e 10 segundos, após quanto tempo de queda livre cada soldado deve acionar o paraquedas? (Cada participante deverá lançar os dados e superar a dificuldade do salto e resolver o problema de tempo)

Possibilidades 1:

1. Superando a dificuldade com os dados e resolvendo o problema, o participante realizará o desafio com sucesso.

2. Caso o participante consiga somente uma das partes do desafio: ~~Ele~~ conseguiu pular, porém o tempo ou destreza foram imprecisos, por isso a consequência foi uma fratura no braço esquerdo. [-1 dano]

3. Caso o participante não acerte nenhuma das partes do desafio: uma pessoa do grupo que obteve êxito deverá instruir corretamente como resolver o problema para que o salto seja feito.

Desafio 2:

Com todos em terra firme, a missão deve prosseguir. O próximo passo é invadir a base alemã. Esta tarefa deve ser realizada com o máximo de cuidado, sem deixar rastros. A

vegetação ao redor do local é mata densa a meia altura e é necessária uma estratégia de aproximação adequada que será decidida pelos soldados. (Voz para os participantes[1]).

Ao decidirem o método de aproximação, os participantes devem lançar os dados para verificar o sucesso da ação de infiltração, que tem nível de dificuldade: fácil (qualquer valor do dado).

Possibilidades 2:

1. Superando a dificuldade com os dados: o participante realizará o desafio com sucesso, se infiltrando na base inimiga

2. Caso o participante não consiga superar o desafio: Ele ficou para trás e os demais participantes devem decidir o que fazer.

2.1 Caso resolvam deixar o companheiro para trás, uma mensagem automática chegará em seus comunicadores de rádio: é o seu general que está comunicando que abandonar companheiros de guerra é equivalente às práticas nazistas, e severas consequências podem acontecer.

2.2 Caso resolvam voltar para resgatar o(s) companheiros é necessário superar o desafio nos dados, novamente ou responder a pergunta : O que é criptografia?

Desafio 3:

Vocês conseguiram invadir a base alemã, lá existem alojamentos, fogueiras, vigias e possui um rio próximo da base também. Vocês conseguiram chegar próximo ao cativeiro, porém o sistema de alarme soou inesperadamente fazendo com que um gás tóxico fosse lançado por toda parte e os reforços do exército inimigo podem chegar a qualquer momento. O gás não é mortífero, mas deixa sequelas graves dependendo do local que conseguiu atingir. Os participantes deverão lançar os dados para escapar. Com isso, a **dificuldade** para esta ação é difícil.

Possibilidades 3:

1. As dificuldades para escapar foram superadas por todos os participantes: todos saem da base inimiga porém não conseguiram realizar o resgate dos prisioneiros.

2. Nem todos conseguiram, através dos dados, escapar do gás totalmente: com isso, estes soldados escaparam, mas foram feridos com o gás na região dos olhos. [-2 dano] Um dos soldados encontrou uma caixa de medicamentos que só é aberta com o código correto.

(Voz para os participantes)

2.1 Os participantes irão tentar desvendar o código da caixa de medicamentos, que tem por codificação: JXHUUD, que pode ser desvendada através do Código de César (tabela fornecida pelo mestre), para assim ser aberta e ter acesso aos medicamentos necessários.

[1] A expressão *voz para os participantes* significa dizer que o jogador deverá decidir, relacionar, organizar seus pensamentos e ideias para executar determinada ação.

2.1.1 Vocês conseguiram abrir a caixa e ajudaram os companheiros feridos, dentro da caixa também havia máscaras de gás que os tornam imunes ao gás tóxico. Todos estão aliviados pois seus amigos acabaram de escapar do perigo, porém a missão ainda não foi completada. Uma informação importante é que um dos soldados avistou o local do cativeiro e já consegue guiar todos diretamente pra lá. Vocês precisam decidir entre continuar a missão e voltar para o esconderijo para salvar os aliados ou retornar para cuidar melhor dos feridos.

Os participantes optaram em prosseguir a missão com os soldados feridos, deste modo, a missão continua com X soldados com a região dos olhos ferida:

2.1.2 Vocês não conseguiram descobrir o código de césar, jogue os dados com o nível de dificuldade mediana para receber ajuda do General sobre o que fazer. Jogada com sucesso: general fornece as três primeiras letras originais.

Desafio 4:

Os soldados viram o local em que estão os reféns em cativeiro, todos deverão tomar cuidado para não despertar suspeitas. Chegando lá, a porta é fechada com dois cadeados que se abrem com uma chave de codificação do método RSA. Os primos p e q que são os escolhidos para essa chave *(verificar antes se eles lembram disto)* estão escritos na gola da camisa do vigilante supremo do cativeiro com os reféns. Ele está a cerca de 100 metros do cativeiro.

(Voz para os participantes)

Possibilidades de falas:

1. Os jogadores escolherem que determinada parte do grupo ficará de vigia no cativeiro e outra parte irá tentar buscar os números desejados.
2. Todos os jogadores vão até o vigilante.
3. Os jogadores tentam conseguir algum material antes de ir até o vigilante ou tentam executar qualquer outra ação até chegar no vigilante.

Em qualquer um dos casos, os jogadores irão precisar jogar os dados para conseguirem realizar tal ação. O nível de **dificuldade** para esta etapa é **fácil**.

Todos devem obter sucesso em qualquer que seja a escolha.

Subitamente, o vigilante consegue detectar que vocês são invasores e vai em direção a vocês para um ataque, ele possui uma arma de fogo e uma granada.

Possibilidades 4:

1.1 Os participantes certamente tentarão atacar também, como o grupo está dividido haverá feridos [-2 dano], mas conseguirão saber os números para a chave. O nível de **dificuldade** para ataque é **mediano**. (Caso o grupo tenha levado os soldados feridos pelo gás, estes perderão alguma parte do corpo, exemplo: braço ou orelha. *eles não poderiam ter ficado de vigia, pois estão com os olhos feridos).

2.1 Se todos os jogadores vão até o vigilante, o vigilante consegue detectar que vocês são invasores e vai em direção a vocês para um ataque, ele possui uma arma e uma

granada. Além disso, seis inimigos aparecem para ajudar o vigilante e vocês terão que se livrar deles para descobrir os números desejados. O **nível** de ataque é **mediano,** porém pode variar de acordo com o número de feridos. É necessário que o grupo consiga os números para a chave.

3.1 O vigilante consegue detectar que vocês são invasores e vai em direção a vocês para um ataque, ele possui uma arma e uma granada. Os jogadores estão com armas, porém como não desejam levantar suspeitas devem ser muito discretos. O vigilante vai em direção ao grupo e ataca, porém como o número de soldados invasores é maior e possui mais armas, o grupo consegue verificar os números da chave com uma facilidade maior. Para executar as ações, vocês deverão jogar os dados em **nível fácil** e no caso de mais inimigos aparecerem, decidam o que farão para voltar ao cativeiro com os números primos. (Esta última ação não será primordial, apenas poderá perder vitalidade, mas não altera o rumo da história).

*Caso os jogadores não tenham conseguido a caixa de medicamentos, conseguirão nessa parte, pois precisarão esconder o vigia em alguma sala. Lembrando que eles devem descriptografar a caixa como no item 2.1 do desafio 3.

Cena 2: Libertação das forças francesas

Com os valores de p e q em mãos, os jogadores poderão voltar ao cativeiro a pé, porém já está amanhecendo e todo cuidado é essencial para que eles possam chegar próximo ao cativeiro novamente. Seguindo um caminho diferente para não levantar suspeitas, os jogadores resolveram retornar através de uma estrada de barro que fica relativamente próxima à base inimiga. Como paisagem, poderão avistar algumas montanhas e árvores grandes. Após algum tempo de caminhada, vocês poderão ver também uma placa informando que o rio Danúbio fica a cerca de 6 km da base. Chegando próximo ao cativeiro por volta das 3h da manhã, vocês podem notar que no entorno do local existe uma intensa movimentação de soldados e veículos alemães. Em um lugar próximo ao que vocês estão há uma escavação na terra, fruto de uma tentativa de fuga de um dos prisioneiros. Essa escavação vai até um lugar que fica apenas a 5 metros do local desejado. Todos devem seguir por este local e é interessante que usem as máscaras que conseguiram na caixa de medicamentos ou na luta com o vigia, por conta da terra e poeira presente na escavação. A **dificuldade** para esta ação é **fácil**, os jogadores devem lançar os dados.

Todos conseguem chegar ao outro lado da escavação sem levantar suspeitas.

Vocês vão aguardar a troca de turno dos vigilantes durante a noite e aproveitarão o momento para tentar utilizar a chave e abrir o cadeado do portão que existe no cativeiro.

Desafio 5: Qual o valor da chave que abre os cadeados? (chave $n = p.q$) , deixar que eles lembrem).

Parabéns! O cadeado foi aberto e vocês finalmente conseguiram entrar no cativeiro dos aliados franceses. Ao entrarem nas celas vocês notam que restaram cerca de 30 soldados franceses e que os mesmos estão muito feridos, além de fragilizados pelas torturas e fome que vêm passando durante os dias de prisão.

Desafio 6: É necessária uma ação de fuga bem planejada e executada para que o inimigo não note a movimentação. Vocês devem fugir silenciosamente do local e saberão que estarão

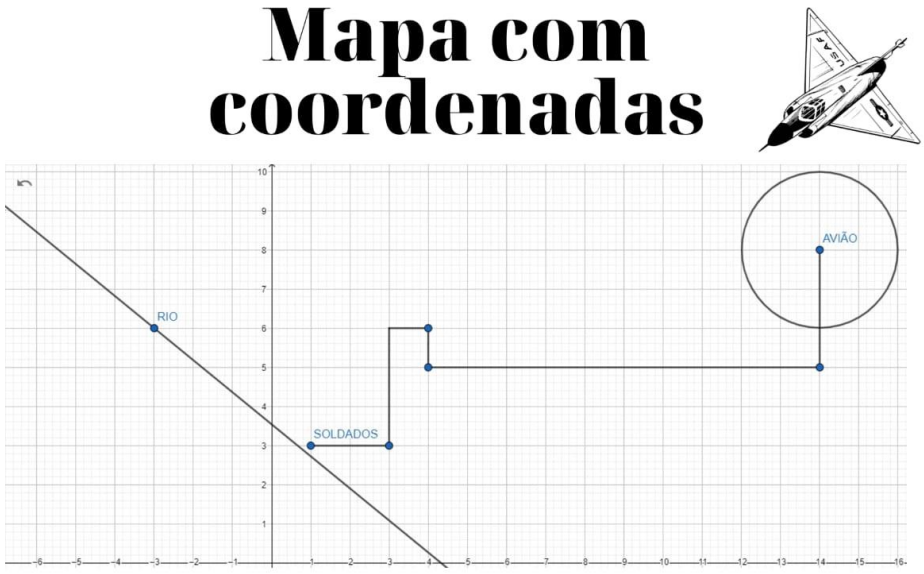
seguros da detecção inimiga quando deixarem a área de alojamento. Para isso é necessário uma rota de fuga que não exponha o grupo que está muito maior agora. O mapa que possui a área total do local está com o general e vocês tentarão entrar com contato com ele para pedir uma dica de fuga adequada. Os jogadores devem lançar os dados para a tentativa de contato com o general. Nível de **dificuldade**: **fácil**.

> Ao conseguirem contato, recebem a seguinte mensagem: "Bravos soldados, vocês conseguiram realizar uma parte da missão libertando os aliados franceses. Analisando o mapa, identifiquei um rio afluente que se encontra com o rio Danúbio mais adiante, 6 km aproximadamente. Este pode servir como boa alternativa para fugirem despercebidos, pois tem correnteza leve e profundidade suficiente para uma camuflagem. No ponto de encontro do afluente com o rio Danúbio será possível encontrar as coordenadas do seu avião cargueiro B 29 Superfortress, que os levarão de volta para a Inglaterra".

Cena 3: Contra-tempo, mudança de planos

O trajeto no rio foi complicado pois vocês tiveram que andar aproximadamente 6 km dentro d'água enfrentando frio e cansaço, contudo foi possível ao chegar no ponto especificado pelo general, encontrar um recipiente amarrado e envolto num plástico com uma mensagem contendo as informações das coordenadas necessárias para o embarque. (Ver mapa de coordenadas)

Figura 28- Mapa de coordenadas



Fonte: Autora, 2020

Desafio 7: Utilizando o mapa e as coordenadas, em que cada unidade representa 1 km, e sabendo que no grupo existem soldados feridos, vocês devem calcular a distância do trajeto até o avião e pensar na logística até lá. Quantos km deverão ser percorridos?

Devido às circunstâncias e à distância envolvida, vocês deverão descansar por um período de tempo para recuperar as forças e partirem logo em seguida. Após o período de descanso e terem percorrido cerca de 12 km houve uma interferência no rádio comunicador:

era uma mensagem criptografada do exército alemão. A mensagem criptografada foi enviada através da enigma. Vocês devem relembrar o método de codificação da enigma e, com isso, vocês ganharão a decodificação da mensagem e saberão o próximo passo do inimigo.

(Voz aos participantes)

Vocês conseguiram descriptografar a mensagem com sucesso! Porém, para a surpresa de vocês, os alemães comunicaram no rádio que haviam descoberto o local estratégico do avião cargueiro B 29 Superfortress e estariam enviando uma frota de caças para o bombardeio e extermínio imediato do avião, acabando com as chances daquilo que seria a oportunidade perfeita para que vocês concluíssem a missão. Minutos depois, foi possível ver no horizonte a fumaça do avião que foi completamente destroçado pelo bombardeio dos caças.

Desafio 8: Com a nova notícia, uma mudança de planos se faz necessária. O transporte que antes era certo, agora não existe mais e vocês estão no meio do território inimigo. Porém, existe uma última esperança: na mensagem inimiga que foi interceptada, uma informação extra surgiu: havia uma tropa se deslocando para uma área de combate, onde iriam transportar mais de 200 soldados num avião cargueiro japonês. Muita atenção neste momento, (ilustrar no quadro), esta tropa seguiria pela estrada, que tem 4km de extensão ao norte e 3km a oeste. Vocês devem calcular a distância para um atalho, fazendo com que suas tropas cheguem ao avião antes da tropa inimiga, surpreendendo os pilotos e tomando o avião para sua própria fuga. Qual será a distância do atalho?

Dada a resposta correta, vocês percorreram o atalho e chegaram rapidamente ao avião japonês. Neste momento vocês precisam realizar uma ação de combate aos pilotos inimigos. Joguem os dados e o nível de **dificuldade** é **mediana**.

*Caso eles não consigam, apenas aumentará o número de feridos.

Desafio 9:

Ao vencerem a disputa com os japoneses, vocês assumem o comando do avião e partem imediatamente para a Inglaterra, onde têm apoio aliado. Contudo, uma nova estratégia é necessária, vocês devem lembrar que estão a bordo de um avião japonês que faz parte das forças do Eixo e, ao entrarem em território inglês, existe o risco de serem abatidos. Desta forma, vocês deverão enviar uma mensagem através do equipamento de rádio informando a hora que o avião em questão chegará na base aliada, um detalhe importante é que esse horário será enviado com a utilização de congruência modular. (Relembrar algum exemplo e fornecer o horário (3h)).

Cena final: Reconhecimento e paz para os povos

Feita esta ação, a mensagem foi recebida com êxito pelos aliados e o desembarque foi bem sucedido em terras inglesas e com isso a missão foi concluída de maneira heróica e honrosa. Agora os soldados de elite são convocados pelo general para receberem as medalhas de honra ao mérito e reconhecimento pelo trabalho feito. Durante a premiação havia mais de 15 mil soldados ovacionando os bravos combatentes e comemorando a vitória conquistada pelos companheiros.

A segunda guerra mundial gerou várias mortes, ocasionando muita dor e sofrimento para as nações e o mundo de forma geral. Percebe-se a importância de manter os países em união para promover um ambiente de paz e de respeito entre os povos. A luta pela paz

permanece até os dias atuais e é dever do ser humano usar da compreensão mútua e da empatia, para respeitar as religiões, raças, povos, crenças em prol de um mundo melhor.

“Nunca houve uma guerra boa, ou uma paz ruim” - Benjamin Franklin