UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

EDMARCOS MARTINS JORDÃO

RSA-CrypTa: UMA APLICAÇÃO DA CRIPTOGRAFIA NO ENSINO MÉDIO

Juazeiro - BA

2023

EDMARCOS MARTINS JORDÃO

RSA-CrypTa: UMA APLICAÇÃO DA CRIPTOGRAFIA NO ENSINO MÉDIO

Dissertação de mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT – UNIVASF como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Edson Leite Araújo

Juazeiro – BA

2023

Jordão, Edmarcos Martins
J82r RSA-CrypTa: uma aplicação da criptografia no ensino médio / Edmarcos Martins Jordão. – Juazeiro-BA, 2023.
xv, 84 f.: il. 29 cm..

Dissertação - (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal do Vale do São Francisco, Campus Juazeiro, 2023.

Orientador: Prof.º Dr.º Edson Leite Araújo.

Inclui referências, apêndice.

1. Matemática - Estudo e ensino. 2. Jogos educativos. 3. Criptografia de dados (Computação). I. Título. II. Araújo, Edson Leite. III. Universidade Federal do Vale do São Francisco.

CDD 510.07

Ficha catalográfica elaborada pelo Sistema Integrado de Biblioteca SIBI/UNIVASF
Bibliotecária: Andressa Lais Machado de Matos CRB – 4/2240

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

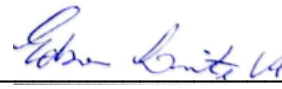
EDMARCOS MARTINS JORDÃO

RSA-CrypTa: UMA APLICAÇÃO DA CRIPTOGRAFIA NO ENSINO MÉDIO

Dissertação de mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UNIVASF como requisito parcial para obtenção do título de Mestre em Matemática.

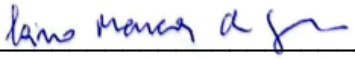
Aprovado em: 28 de agosto de 2023.

Banca Examinadora



Prof. Dr. Edson Leite Araújo

Orientador – PROFMAT/UNIVASF.



(Prof. Dr. Lino Marcos da Silva

Examinador Interno: PROFMAT/UNIVASF

(Profa. Dra. Carla Saturnina Ramos de Moura

Examinadora Externa: UPE

À Deus, pela oportunidade de viver.

AGRADECIMENTOS

A Deus pela força para perseverar!
Ao Prof. Dr. Edson Leite Araújo, pela excelente orientação.
Aos colegas da turma pelo incentivo e união.

"A matemática é arte, o resto é fazer conta."

RESUMO

O advento da internet, o avanço da tecnologia e das comunicações trouxeram mais conforto e comodidade ao ser humano e como consequência veio a necessidade de privacidade e proteção de informações, requisitos conquistados com o desenvolvimento e implementação de métodos eficazes de criptografia, área da computação cujos fundamentos apoiam-se em vários conceitos matemáticos. Entre as técnicas existentes, a RSA (Rivest-Shamir-Adleman) tem sido a mais segura e utilizada. Com o intuito de contribuir com o ensino dos conteúdos matemáticos relacionados, como mínimo múltiplo comum, máximo divisor comum, números primos e equação diofantina, este trabalho propõe uma alternativa de ensino-aprendizagem de maneira lúdica, explorando tais conceitos através de um jogo online sobre a criptografia RSA, oportunizando os primeiros contatos para alunos do nível médio, com uma aplicação real, dos conceitos matemáticos envolvidos. Tal jogo simula a interceptação de uma troca de mensagens criptografadas usando RSA onde, em etapas como fases do jogo, tenta-se a desencriptação, explorando em cada uma, os conceitos matemáticos necessários para tanto. Essa abordagem interativa e prática tem se mostrado eficiente, com um rendimento de 81,3% dos alunos que participaram do jogo em comparação com apenas 53% daqueles que não tiveram essa vivência, bem como uma percepção positiva do aplicativo superior a 86%.

Palavras-chave: Ensino de Matemática. Números Primos. Descriptografia. Sistema RSA. Jogo online.

ABSTRACT

The advent of the internet, advances in technology, and communications have brought more comfort and convenience to humankind, consequently creating a need for privacy and information protection. These requirements have been achieved through the development and implementation of effective encryption methods, which are based on various mathematical concepts within the field of computer science. Among the existing techniques, RSA has proven to be the most secure and widely utilized. With the aim of contributing to the teaching of related mathematical contents such as least common multiple, greatest common divisor, prime numbers, and Diophantine equation, this study proposes an alternative approach to teaching and learning in a playful manner. It explores these concepts through an online game focusing on RSA encryption, providing initial exposure to high school students regarding the real-world applications of the mathematical concepts involved. This game simulates the interception of RSA-encrypted message exchanges, and within each stage or level, decryption is attempted while exploring the necessary mathematical concepts. This interactive and practical approach has proven to be efficient, with an achievement rate of 81.3% among students who participated in the game, compared to only 53% among those who did not have this experience. Additionally, the application has garnered a positive perception rate exceeding 86%.

Keywords: Mathematics Teaching. Prime Numbers. Decryption. RSA system. Online game.

LISTAS DE FIGURAS

LISTA DE GRÁFICOS

LISTAS DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES	Advanced Encryption Standard
CAST	Carlisle Adams and Stafford Tavares
DES	Data Encryption Standart
IDEA	International Data Encryption Algorithm 2
MDC	Máximo Divisor Comum
MIT	Massachusetts Institute of Technology
MMC	Mínimo Múltiplo Comum
PISA	Programa Internacional de Avaliação de Estudantes
RC2	Rivest Cipher 2 ou Ron's Code 2
RSA	R. L. Rivest, A. Shamir, L. Adleman
DCRB	Documento Curricular Referencial da Bahia
PcD	Pessoa com Deficiência

LISTA DE SÍMBOLOS

$\mathbb{R}$	Conjunto dos Números Reais
$\mathbb{N}$	Conjunto dos Números Naturais
$\varphi(n)$	Função Phi

SUMÁRIO

1 INTRODUÇÃO

Cada vez mais, a sociedade depende da comunicação mediada por dispositivos eletrônicos conectados à internet. Entre janeiro de 2012 e o mesmo mês em 2022, houve um aumento em mais de 50% no número de internautas no mundo, alcançando a quantidade de 4,95 bilhões de usuários (Datareportal, 2022).

Através do acesso à rede mundial de computadores, são realizadas atividades diversas, como ensino, entretenimento, transações comerciais ou bancárias, promovendo a conexão entre pessoas, entre instituições, entre pessoas e instituições, preservando-se as informações envolvidas, com destaque àquelas que não se deseja tornar públicas (Kurose; Ross, 2013).

Neste ambiente, são comuns ataques hackers à empresas, pessoas públicas ou anônimas, em geral com intuito de natureza ilícita, como os crimes financeiros, por exemplo. Nesse sentido, existem algumas formas simples, embora não sejam tão eficazes, de proteção como evitar o uso de aparelhos por terceiros ou de redes abertas. No entanto, a forma mais usada para a proteção de vazamentos indesejados se dá através do uso de técnicas de criptografia (Oliveira, 2012).

Um dos casos históricos mais famosos de uso da *criptografia* é o da *máquina Enigma*, projetada pelos nazistas durante a segunda guerra mundial, com o objetivo de promover a comunicação com suas tropas em combate, de modo seguro e privativo. Em seu livro, Leavitt (2015), narra a saga de Alan Turing, matemático britânico, ao tentar descriptografar mensagens enviadas às tropas alemãs utilizando a *Enigma*. A participação do matemático foi crucial para a derrota das tropas nazistas, uma vez que graças à técnica de decodificação desenvolvida por ele, os Aliados[1] puderam se antecipar às investidas alemãs e obter vantagens nos confrontos. Desde então as técnicas criptográficas vêm se sofisticando e tornando-se cada vez mais eficientes, impossibilitando que sejam quebradas com facilidade (Stallings, 2014). Outros casos interessantes podem ser encontrados em Singh (1999).

Entre as inúmeras técnicas existentes na literatura, uma das mais seguras e utilizadas é a RSA - batizada assim em homenagem aos seus criadores, R. L.

[1] Durante a Segunda Guerra mundial, os Aliados eram um grupo de países formado pelo Reino Unido, França, União Soviética e Estados Unidos que enfrentavam as forças do Eixo, compostas por Alemanha, Itália e Japão.

Rivest, A. **S**hamir e L. **A**dleman (Coutinho, 2014). Essa técnica de criptografia usa conceitos matemáticos estudados desde o século XVII, a maior parte presente no currículo escolar do ensino fundamental (Biachini, 2018) e médio (Bonjorno *et al* 2020). Entre estes, estão conteúdos como *mínimo múltiplo comum*, *máximo divisor comum*, *números primos* e *fatoração*, importantes para o entendimento da *aritmética modular* (Coutinho, 2014). Já existe inclusive, um livro didático (Selk, 2020), que trata da *criptografia* no ensino médio.

No século XIX, nomes como *Fermat*, *Euler*, *Gauss* e *Riemann*, estudaram aspectos ligados aos *números primos*, sem quaisquer finalidades práticas aparentes, utilizando-os apenas como parte do exercício matemático das descobertas, quando no século XX, foram enfim usados para objetivos práticos, entre os quais está a *criptografia RSA* (Coutinho, 2014).

Na *Escola Estadual de Tempo Integral Manoel Novaes* em Curaçá-Ba, um dos grandes desafios, além de atrair a atenção dos alunos, é o controle do celular em sala de aula. Diversas reuniões e conselhos de classe já foram estabelecidos com o propósito de discutir mecanismos de controle desses aparelhos por parte do aluno, de forma que não atrapalhe ou, até mesmo que possam auxiliar a compreensão dos conteúdos planejados. Com as redes sociais, jogos digitais e inteligências artificiais, torna-se a cada dia, mais difícil atrair a atenção dos estudantes através de aulas tradicionais. Aliado a isso e à intenção de proporcionar um modelo de ensino que exiba a matemática aplicada ao mundo moderno, é que se pensou e criou, como ferramenta de aprendizagem, um jogo online utilizando a *criptografia RSA* com a finalidade de ensinar de forma lúdica e divertida conteúdos matemáticos ligados ao seu funcionamento e que também façam parte da grade curricular dos alunos no ensino básico.

Segundo Almeida (2011), é comum aos alunos, questionarem o ensino de conteúdos matemáticos, alcançando inclusive a desmotivação por não enxergarem aplicações relacionadas e úteis em seu cotidiano ou que expliquem fatos presentes em suas vidas. Somdo a isto, dados publicados pelo Pisa (2019), afirmam que 68,1% dos estudantes brasileiros em 2018 se encontram no Nível 1 ou abaixo dele[2], nos requisitos referentes a matemática.

[2] Abaixo do Nível 1: Estudantes que se quer alcançaram as habilidades necessárias ao Nível 1.

Tem-se discutido no meio educacional (Silva e Cunha, 2012; Pasdiora, 2008; Madeira *et al,* 2015) o papel dos jogos eletrônicos para fins didáticos com a pretensão de serem lúdicos, atrativos e alcançar em um aprendizado eficiente. Nesse sentido, Albuquerque e Fialho (2009, p.1-2) destacam que:

> O jogo eletrônico é projetado nos mínimos detalhes, e oferece ao jogador não apenas um sistema de regras, mas personagens, ambientações e sistemas de regras complexas calculadas em tempo infinitamente pequeno. E oculto nesse emaranhado de informações, um conteúdo a ser aprendido, (...) A interatividade dos jogos eletrônicos exige um comportamento ativo do jogador. O desafio do jogo exige um investimento de energia mental que posiciona o jogador em um nível mais elevado de interação: o aprendizado sobre algo que ele influencia ativamente possibilita não apenas que ele perceba o contexto por outro ponto de vista, mas que desenvolva a habilidade de resolver outros problemas relacionados ao conteúdo em questão.

Configuram, portanto, uma possibilidade de aprendizagem matemática potencializada pelo interesse que desperta no jogador em conexão à sua participação como ser ativo e o ambiente atrativo que o motivam a prosseguir e aprender mais a cada etapa em que se evolui no jogo.

Embora existam muitos trabalhos sobre esse tema (Bruxelas, 2021; Silva, 2019), uma verificação no acervo online de dissertações do PROFMAT até 2021, revela que, apesar de uma delas (Luz, 2013) trazer uma proposta de aplicativo que usa comandos no Máxima para implementar o RSA (mais informações sobre o Máxima podem ser obtidas no site: https://maxima.sourceforge.io/) e outra (Souza, 2020) apresentar uma sequência didática para ser usada como minicurso ou disciplina eletiva para alunos do Ensino Médio - nenhum chega a ser finalizado e implantado eletronicamente. Há, porém, o trabalho de Silva (2021) que traz uma simulação em rede social de uma aplicação do RSA, mas não chega a implementá-la ou mesmo aplicá-la. Constata-se, portanto, a carência de trabalhos no PROFMAT que tratem do tema com o uso de aplicativos especificamente projetados para fins didáticos, em sala de aula, seja em versão de esboço ou mesmo definitiva.

Este trabalho tem, portanto, como objetivo geral:

- Implementar um jogo em ambiente online que simule a interceptação de uma troca de mensagens privadas protegidas através do sistema

de *criptografia RSA*, para uso em sala de aula, exibindo no processo de quebra da proteção, como fases do jogo, a exploração de conteúdos matemáticos como o *mmc, mdc*, *números primos* e *equação diofantina* para criptografar (codificar) e descriptografar (decodificar) mensagens.

Como objetivos específicos, espera-se:

- Analisar possíveis potencialidades do jogo na aprendizagem dos conteúdos abordados.
- Motivar e despertar a curiosidade dos alunos a se aprofundarem em conteúdos matemáticos aplicáveis nas tecnologias digitais.
- Mostrar aos alunos um exemplo de aplicação da matemática no mundo moderno.
- Construir uma sequência didática que use o jogo e que explore os conteúdos de soma, subtração, multiplicação e divisão de números inteiros, mmc, mdc, números primos, equação diofantina em paralelo a equação e função do primeiro grau, e pensamento lógico dedutivo.

Pretende-se apresentar os conteúdos utilizando como recursos um jogo online denominado por nós de **RSA-CrypTa**, começando no capítulo 02 por apresentar aspectos da criptografia e seus fundamentos. Nesse capítulo, é retratado como foram os primeiros usos da criptografia, as técnicas e algoritmos mais usados atualmente incluindo, o RSA.

O Capítulo 3 aprofunda-se no sistema RSA, discorrendo sobre suas origens, criadores e o funcionamento geral, incluindo a matemática envolvida para a codificação e decodificação de mensagens. Além disso, são exibidas aplicações desse sistema. O capítulo oferece uma explicação detalhada dos processos matemáticos envolvidos em cada etapa, auxiliando o leitor a compreender a robustez e segurança do sistema.

No Capítulo 4, é apresentado o jogo **RSA-CrypTa**, incluindo seu funcionamento e sua aplicabilidade no contexto escolar. O jogo é projetado para promover uma assimilação mais eficiente e lúdica dos conteúdos matemáticos ao

mesmo tempo em que exemplifica a aplicação da matemática no mundo moderno, despertando a curiosidade e favorecendo a aprendizagem. Neste mesmo capítulo também é apresentada a metodologia para a exibição e utilização do aplicativo em sala de aula.

Os resultados acerca das atividades realizadas com os alunos, são discutidos no Capítulo 5. Por fim, o Capítulo 6 apresenta as conclusões e reflexões pessoais acerca dos resultados obtidos, fornecendo uma visão do estudo.

2 CRIPTOGRAFIA E SEUS FUNDAMENTOS

Durante toda a história humana em sociedade organizada, houve a necessidade de se proteger informações sigilosas. Esconder apenas, não era o bastante para proteger o conteúdo de uma mensagem e muitas vezes a ampliação dessa proteção foi feita através de modificações na forma de escrevê-la, como o embaralhamento de letras ou substituição por outras, com a finalidade de confundir seu entendimento para aqueles com acesso não autorizado. Todavia, esse tipo de proteção se mostrou precário e por diversas vezes violável com certa facilidade (Fiarresga, 2010).

Os primeiros registros sobre o uso da *criptografia* foram encontrados no Egito antigo, por volta de 1900 a.C, no túmulo de Khnumhotep II, na vila de Menet Khufu. Outros povos antigos da mesma época também se utilizavam desses recursos para camuflarem suas mensagens (Fiarresga, 2010).

A finalidade da *criptografia* é portanto, tornar incompreensível a leitura não autorizada de uma mensagem. Como afirma Coutinho (2015, p.1): “A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la”. Em consequência, *uma mensagem pode estar em mãos não autorizadas, desde que a compreensão de seu conteúdo não seja possível.*

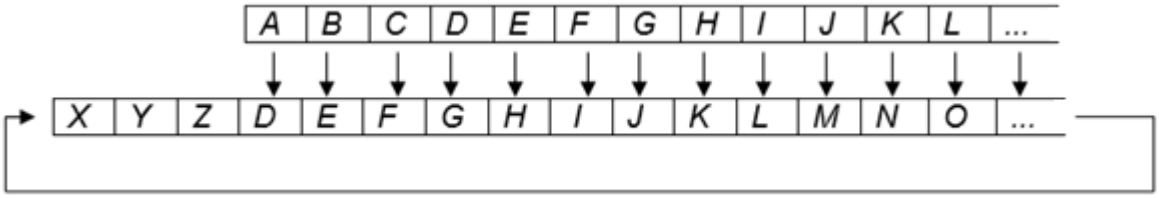
Um dos usos mais comuns da camuflagem de mensagens ocorre para objetivos militares, desde o século V a.C. Um exemplo que merece destaque é a *cítala dos espartanos* (Figura 01), que consistia no uso de um *bastão* de formato, tamanho e diâmetro variados, mas que cada interlocutor tinha o seu no formato e tamanho previamente combinados entre eles, no qual era enrolado uma *fita* fina, que podia ser de *couro*, contendo uma mensagem embaralhada. Fora do bastão, a fita de leitura era apenas uma espécie de cinto com uma escrita confusa, letras fora de ordem e incompreensível. Porém, quando enrolada no bastão adequado, revelava o seu verdadeiro conteúdo (Fiarresga, 2010).

Figura 01: Cítala dos espartanos

Fonte: (Fiarresga, 2010)

Com o tempo, surgiram outras técnicas, como a *Cifra de César*, imperador romano, em 50 a.C, que consistia basicamente em trocar a posição das letras do alfabeto (Figura 02) cuja regra de associação de cada posição era previamente combinada entre seus interlocutores (Coutinho, 2015). Sendo assim, possibilitava a encriptação de mensagens mais longas, já que a *Cítala* não comportava tantas informações, além de não depender de um bastão.

Figura 02: Cifra de César



Fonte: Próprio autor

Para Stallings (2014), do ponto de vista matemático, uma boa *criptografia* codifica uma mensagem usando uma *função bijetiva* e portanto, *inversível* que permite que uma mensagem *codificada* também possa ser *decodificada* uma vez conhecido o seu método (a função).

As técnicas criptográficas evoluíram bastante ao longo dos séculos tendo em vista a necessidade de tornarem-se mais fortes e seguras, chegando atualmente a dois tipos básicos: *simétricas* e *assimétricas*. Ambas necessitam de *chaves*, que correspondem a códigos de acesso à mensagem ou, de forma mais usual, senhas de acesso.

A *criptografia simétrica* necessita de uma *chave única*, ou também conhecida como *chave privada*, que é usada tanto para *codificar* quanto para *decodificar* a mensagem. Ao passo que a *assimétrica* usa duas chaves: uma para *codificar*, que é de *conhecimento público*, e a outra para *decodificar*, que é *privada*. É interessante destacar que, apesar de serem diferentes em essência, ambos os tipos de criptografias podem ser usados em diferentes situações ou mesmo juntas, sendo portanto, inapropriado afirmar que uma é melhor do que a outra (Oliveira, 2012).

Segundo Oliveira (2012), a escolha de um tipo ou outro de *criptografia* depende do contexto e em alguns casos o uso de ambas pode ser bem mais proveitoso.

A *criptografia simétrica* possui a vantagem de ser mais simples, de implementação rápida e menos complexa, já que exige um poder menor de processamento. Entretanto, possui as desvantagens de não ter uma boa gerência e distribuição de chaves, além de não permitir o uso de *assinaturas digitais,* que é uma técnica criptográfica que visa confirmar a um dos interlocutores que o outro é realmente quem diz ser. A gerência e distribuição das chaves são certamente grandes problemas, uma vez que se trata de apenas *uma* chave usada tanto para encriptar (codificar) quanto desencriptar (decodificar) uma mensagem. Se em mãos erradas, todo o processo de codificação será em vão. A impossibilidade de proporcionar uma assinatura digital, exclui o sistema de muitas atividades desenvolvidas na rede de computadores. Apesar disto, conta com uma variedade de algoritmos, como: AES, DES, 3 DES, IDEA, Blowfish, Twofish, RC2 ou CAST (Oliveira, 2012).

A *criptografia assimétrica* foi desenvolvida por Whitfiled Diffie e Martin Hellman, ambos da Stanford University, em 1976, muito embora exista uma reivindicação do almirante Bobby Inman, que afirma tê-la desenvolvido antes, na década de 1960. Há também registros do conceito de *chave pública*, ideia central para a *criptografia assimétrica*, em 1970 pela Communications Eletronics Security Group, mas em relatório secreto (Stallings, 2014).

Para Oliveira (2012), o método possui a vantagem de ter uma boa distribuição e gerenciamento de chaves, pois não depende de uma chave única, e oferece assinatura digital. Entretanto, possui a desvantagem de ter um

processamento lento e implementação mais complexa, sendo inviável para alguns tipos de atividades que necessitam maior agilidade.

Apesar de ser mais lenta, a *criptografia assimétrica* é bastante útil nas certificações digitais, além de ser mais apropriada ao tráfego de mensagens online. Contudo, para ter maior eficiência é comum usar nesses tipos de atividades os dois tipos: *simétrico* e *assimétrico*, o chamado sistema *híbrido*. Entre os algoritmos *assimétricos* encontra-se o RSA.

3. O ALGORITMO RSA

A teoria dos números primos é uma das poucas áreas da matemática pura que encontra aplicação direta no mundo real, mais precisamente na *criptografia* (Singh, 1999).

Como dito anteriormente, o processo de *codificação simétrico* envolve o uso de *uma* chave secreta e tradicionalmente a *decodificação* exige que o receptor aplique a mesma chave no sentido inverso. Deste modo, a *chave* é o elo mais fraco no processo.

Na década de 1970, Diffie e Hellman tiveram a ideia de procurar um procedimento matemático que fosse fácil de aplicar num sentido e incrivelmente difícil aplicar no sentido inverso. Nascia assim o conceito de *chave pública* e o método de codificação *assimétrico* (Diffie e Hellman, 1976).

Um ano após Diffie e Hellman introduzirem o conceito de *chave pública,* três jovens matemáticos do Massachusetts Institute of Technology - MIT, Ronald Rivest, Adi Shamir e Leonard Adleman, perceberam que os *números primos* eram a base ideal para a *chave perfeita*. Tal algoritmo ficou conhecido como RSA, que são as iniciais dos nomes dos inventores (Coutinho, 2014).

3.1 COMO FUNCIONA O RSA

O RSA é um sistema de *criptografia assimétrico* que funciona tendo como base o uso de *um par* de chaves: uma *pública* e uma *privada*. São obtidas através da escolha de dois diferentes números primos grandes, p e q, que são multiplicados entre si, gerando um novo número, $n = p \cdot q$. Com o conhecimento dos números $p, q,$ e n e por meio de um processo matemático, chega-se a duas chaves: a *pública,* responsável pela *codificação* e a *privada,* usada para a *decodificação* da mensagem (Stallings, 2014).

Matematicamente, é extremamente difícil decompor o número n nos dois fatores primos que o produziram (isto devido ao fato de p e q terem sido escolhidos muito grandes), tornando o processo extremamente útil aos propósitos criptográficos. Além disso, não existem técnicas eficientemente úteis com totais

garantias de geração de números primos de qualquer tamanho, o que faz com seja necessário o uso de métodos probabilísticos para este fim (Stallings, p. 212, 2014).

O algoritmo RSA é baseado nas seguintes condições: dados dois números primos p e q, escolhe-se um número $m \epsilon \mathbb{N}$ que seja relativamente primo a p e q simultaneamente, ou seja:

$$mdc(m,p) = 1$$
$$mdc(m,q) = 1$$

Em tais condições, o **Teorema de Euler** (Hefez, 2016), garante que:

$$m^{(p-1)(q-1)} \equiv 1\ mod(p \cdot q)$$

Dados dois números e e d, tais que

$$e \cdot d \equiv 1\ mod\big((p-1)(q-1)\big)$$

tem-se que:

$$(m^e)^d\ mod(p \cdot q) = (m^{e \cdot d})\ mod(p \cdot q) = m\ mod(p \cdot q)$$

Ou seja, conhecendo-se m^e (mensagem encriptada), é possível descobrir m (a mensagem) usando d, tendo em vista que

$$(m^e)^d mod(p \cdot q) = m\ mod(p \cdot q)$$

Em outras palavras, se entendermos m como uma *mensagem* que se deseja proteger, de posse do par de números (e,n) (*chave pública*), onde $n = p \cdot q$, tem-se a *mensagem criptografada* dada por

$$m^e\ mod(p \cdot q)$$

e através do par (d,n) (*chave privada*), é possível *desencriptografar*[3] tal mensagem, uma vez que:

$$m = (m^e)^d mod(p \cdot q)$$

[3] A escolha das letras e e d, se explica por significarem “encriptação” e “desencriptação”, respectivamente.

3.2 AS OPERAÇÕES

A encriptação *assimétrica*, entre elas o RSA, precisa obedecer a algumas regras:

- Para funcionar:

  (F_1) Ter um algoritmo para *encriptação* usando a chave pública, e um algoritmo relacionado, para *decriptação* usando a chave privada.

  (F_2) O emissor e o receptor precisam ter, cada um, sua respectiva chave.

- Para a segurança:

  (S_1) Uma das duas chaves precisa permanecer secreta.

  (S_2) Deverá ser impossível, ou pelo menos impraticável, decifrar uma mensagem com uma das chaves mantida secreta.

  (S_3) O conhecimento do algoritmo, uma das chaves e amostras do texto cifrado, devem ser insuficientes para determinar a outra chave.

3.2.1 A geração das chaves

O processo de geração das chaves, *pública* (e, n) e *privada* (d, n), obedece ao seguinte roteiro:

(G_1) Escolher dois grandes números primos quaisquer, p e q, com $p \neq q$ e atribuir $n = p \cdot q$. Como não existem até o momento da escrita deste trabalho, métodos eficazes para a geração de números primos, tal escolha em geral é feita usando algoritmos determinísticos como o Miller-Rabin (Stallings, p. 189, 2014).

(G_2) Gerar o número $\varphi(n) = (p-1)(q-1)$, também conhecida como *função Totiente de Euler*.

(G_3) Escolher $e, d \in \mathbb{N}$, tal que $1 < e < \varphi(n)$, $e \cdot d \equiv 1\ mod(\varphi(n))$ e que seja có-primo com $\varphi(n)$, ou seja, $mdc(\varphi(n), e) = 1$.

Isto requer algumas tentativas e erros. Inicialmente o número e é escolhido aleatoriamente. O **Algoritmo de Euclides** é usado para encontrar

$$mdc(e, \varphi(n)) = 1$$

e em seguida resolve-se a equação diofantina:

$$e \cdot x + \varphi(n) \cdot y = 1$$

onde $d = x$. Deste modo, tem-se que:

$$e \cdot d - 1 = -y \cdot \varphi(n) \Longrightarrow e \cdot d \equiv 1 \, mod \, \varphi(n).$$

(G_4) Escolher um alfabeto[4] para codificar as letras em números. Um exemplo é dado na Figura 03.

Figura 03: Exemplo de alfabeto em código numérico

10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*L*	*M*	*N*

23	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**
O	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*X*	*Z*	*W*	*Y*	*K*

Fonte: Próprio autor

O procedimento feito em (G_1) tem a finalidade de encontrar candidatos p e q primos que, quando adquiridos, deverão ainda obedecer aos cuidados:

(C_1) p e q deverão diferir em tamanho por apenas alguns dígitos decimais. Assim, para uma chave de 1024 bits (309 dígitos decimais), tanto p como q deverão estar na ordem de grandeza de 10^{75} (249 bits) a 10^{100} (332 bits), o que corresponde a uma diferença

[4] O alfabeto neste caso, trata-se de uma associação entre letras e números e é passado previamente às partes envolvidas. Por exemplo: no alfabeto aqui escolhido, a letra A está associada ao número 10. Há, portanto, diversas possibilidades de tipos de alfabetos que podem ser utilizados. O alfabeto ASCII completo ou uma versão modificada, disponível no link https://www.asciitable.com/, é usado como alfabeto padrão, a partir do qual, outros alfabetos são criados.

de 25 dígitos decimais ou 83 bits. Isso garante que ambos os números p e q sejam grandes.

(C_2) Tanto $(p-1)$ quanto $(q-1)$ deverão conter um fator primo grande cada e $mdc(p-1, q-1)$ deve ser pequeno.
Se os fatores primos forem pequenos, torna-se fácil a fatoração de n, por conseguinte, a obtenção de p e q que culminará na descoberta da chave privada.

Para melhor compreensão, observe como proceder para a geração de chaves de 16 bits, no exemplo a seguir:

Exemplo 01: De acordo com (C_1), os primos p e q devem ser escolhidos de modo que a diferença de dígitos entre eles seja pequena, digamos 2 dígitos (binários). Desta forma, por (G_1), recorrendo a uma tabela de primos, escolhemos

$$p = 107 \text{ (7 bits)}$$
$$q = 383 \text{ (9 bits)}$$

Assim,

$$n = p \cdot q$$
$$= 40.981 \text{ (16 bits)}$$

Observe que

$$p - 1 = 106 = 2 \cdot 53$$
$$q - 1 = 382 = 2 \cdot 191$$

Possuem ambos, fatores primos grandes, 53 e 191 respectivamente. Além disso:

$$mdc(p-1, q-1) = 2,$$

respeitando, portanto, (C_2). Seguindo com (G_2), tem-se:

$$\varphi(n) = (p-1) \cdot (q-1)$$
$$= 106 \cdot 382$$
$$= 40.492$$

Para o passo (G_3), é necessário agora escolher e, com $1 < e < \varphi(n)$ e tal que $mdc\left(e, \varphi(n)\right) = 1$. Usando o **Algoritmo de Euclides**, tem-se:

$$e = 40.491$$

Com isto, tem-se a *chave pública*

$$(e, n) = (40.491, 40.981)$$

Para deduzir a *chave privada*, continuamos com o passo (G_3) no qual é necessário encontrar $d\ \epsilon\ \mathbb{N}$ tal que

$$(e \cdot d)\ mod\ \varphi(n) = 1 \Rightarrow$$
$$e \cdot d + y \cdot \varphi(n) = 1 \Rightarrow$$
$$d = 80.983$$

O par $(d, n) = (80.983, 40.981)$ é, portanto, a *chave privada*. ■

3.2.2 Encriptação

De posse dos números e e n, que formam a chave pública:

(E_1) Pré-codificar a mensagem associando cada caractere a um correspondente m pré-estabelecido em um alfabeto (Figura 03).

(E_2) Calcular $c = m^e\ mod(n)$**,** onde c será o número da letra cifrada. Mais detalhes do processo de obtenção de c pode ser encontrado no Exemplo 02.

(E_3) Repetir o passo (E_2) em todos os caracteres da mensagem pré codificada.

As mensagens codificadas são colocadas em pequenos blocos de mesmo tamanho para facilitar o processo de decodificação, uma vez que sem conhecer o tamanho dos blocos formados, pode haver confusão de quais números usar. Por exemplo: Na mensagem codificada como 2345678920, como saber se os números a serem decodificados são o número 2345678920 ou 234, 567 e 8920? Ou 2345, 6789 e 20? São muitas possibilidades e com um tamanho padrão se facilita esse processo (Coutinho, 2014).

Vejamos, no exemplo a seguir, como executar os procedimentos mencionados anteriormente, para encriptar a palavra “**PRIMOS**”.

Exemplo 02: De acordo com o alfabeto escolhido (Figura 03), a letra **P** foi associada ao número $m_p = 24$, e seguindo (E_1) a sua encriptação é dada por

$$c_p = m_p^e \, mod(n)$$

Sendo

$$e = 40491$$
$$n = 40981,$$

de acordo com o que foi feito no Exemplo 01. Ou seja,

$$c_p = 24^{40491} mod(40981)$$

Observe que, mesmo sendo uma codificação em 16 bits, os números e e n são muito grandes e isto é o que acontece no caso geral. Segue-se que, a maneira tradicional de executar esse cálculo não é indicada, sendo portanto, necessária a adoção de algum algoritmo rápido e eficiente para este fim. Neste exemplo vamos utilizar o algoritmo conhecido como **Método dos Quadrados Binários**, pensado em outro contexto por Knuth (1997) e formalizado em (Schneier 2015).

Inicialmente, observe que o expoente e pode ser escrito como soma de potências de 2, da seguinte forma

$$\begin{aligned} e &= 40491 \\ &= 1 + 2 + 2^3 + 2^5 + 2^9 + 2^{10} + 2^{11} + 2^{12} + 2^{15} \end{aligned}$$

O procedimento para se chegar a esta soma é semelhante ao processo de escrever o número e na base 2, ou em outras palavras, em *binário*. Além disto, esta soma terá no máximo 16 termos, uma vez que estamos trabalhando com 16 bits. Assim,

$$\begin{aligned} c_p &= 24^{40491} mod(40981) \\ &= 24^{1+2+2^3+2^5+2^9+2^{10}+2^{11}+2^{12}+2^{15}} mod(40981) \\ &= \left(24 \cdot 24^2 \cdot 24^{2^3} \cdot 24^{2^5} \cdot 24^{2^9} \cdot 24^{2^{10}} \cdot 24^{2^{11}} \cdot 24^{2^{12}} \cdot 24^{2^{15}}\right) mod(40981) \end{aligned}$$

Perceba também que,

$$24\ mod(n) \ = 24$$
$$24^2 mod(n) = 576 mod(n)$$
$$= \ 576$$

$$24^{2^3} mod(n) = 24^{2^2+2^2} mod(n)$$
$$= \left(24^{2^2} mod(n) \cdot 24^{2^2} mod(n)\right) mod(n)$$
$$= (3928 \cdot 3928) mod(n)$$
$$= 20328$$

$$24^{2^5} mod(n) \ = 24^{2^4+2^4} mod(n)$$
$$= \left(24^{2^4} mod(n) \cdot 24^{2^4} mod(n)\right) mod(n)$$
$$= (16161 \cdot 16161) mod(n)$$
$$= \ 6008$$

$$24^{2^9} \ mod(n) = 24^{2^8+2^8} mod(n)$$
$$= \left(24^{2^8} mod(n) \cdot 24^{2^8} mod(n)\right) mod(n)$$
$$= (14688 \cdot 14688) mod(n)$$
$$= \ 13360$$

$$24^{2^{10}} mod(n) = 24^{2^9+2^9} mod(n)$$
$$= \left(24^{2^9} mod(n) \cdot 24^{2^9} mod(n)\right) mod(n)$$
$$= (13360 \cdot 13360) mod(n)$$
$$= \ 17345$$

$$24^{2^{11}} mod(n) = 24^{2^{10}+2^{10}} mod(n)$$
$$= \left(24^{10} mod(n) \cdot 24^{2^{10}} mod(n)\right) mod(n)$$
$$= (17345 \cdot 17345) mod(n)$$
$$= \ 7504$$

$$24^{2^{12}} mod(n) = 24^{2^{11}+2^{11}} mod(n)$$
$$= \left(24^{2^{11}} mod(n) \cdot 24^{2^{11}} mod(n)\right) mod(n)$$
$$= (7504 \cdot 7504) mod(n)$$

$$= 2122$$

$$\begin{aligned} 24^{2^{15}} mod(n) &= 24^{2^{14}+2^{14}} mod(n) \\ &= \left(24^{2^{14}} mod(n) \cdot 24^{2^{14}} mod(n)\right) mod(n) \\ &= (16380 \cdot 16380) mod(n) \\ &= 1793 \end{aligned}$$

Logo,

$$\begin{aligned} c_p &= (24 \cdot 576 \cdot 20328 \cdot 6008 \cdot 13360 \cdot 17345 \cdot 7504 \cdot 2122 \cdot 1793) mod(n) \\ &= ((((24 \cdot 576 \cdot 20328) mod(n)) \cdot 6008 \cdot 13360 \cdot 17345 \cdot 7504 \cdot 2122 \\ &\qquad \cdot 1793) mod(n))\ mod(n) \\ &= ((((7555 \cdot 6008) mod(n)) \cdot 13360 \cdot 17345 \cdot 7504 \cdot 2122 \\ &\qquad \cdot 1793) mod(n))\ mod(n) \\ &= ((((24473 \cdot 13360) mod(n)) \cdot 17345 \cdot 7504 \cdot 2122 \cdot 1793) mod(n))\ mod(n) \\ &= ((((12862 \cdot 17345) mod(n)) \cdot 7504 \cdot 2122 \cdot 1793) mod(n))\ mod(n) \\ &= ((((31807 \cdot 7504) mod(n)) \cdot 2122 \cdot 1793) mod(n))\ mod(n) \\ &= (((6384 \cdot 2122) mod(n)) \cdot 1793)\ mod(n) \\ &= (23118 \cdot 1793)\ mod(n) \\ &= 18783 \end{aligned}$$

Destaca-se que apesar do longo processo, este algoritmo foi comparado quanto à sua velocidade e eficiência com outros dois concorrentes (Bosselaers, Govaerts e Vandewalle 1994) e segundo os autores, possui performance muito próxima aos demais. Duas implementações bastante simples, uma em C e outra em Python, podem ser encontradas no Apêndice A.

Procedendo do mesmo modo para as demais letras da palavra **“PRIMOS”**, tem-se

$$c_r = 26^e mod(n) = 07881$$
$$c_i = 18^e mod(n) = 25044$$
$$c_m = 21^e mod(n) = 03903$$
$$c_0 = 23^e mod(n) = 24945$$
$$c_s = 27^e mod(n) = 16696$$

Portanto, a palavra **“PRIMOS”** é encriptada como

18783 07881 25044 03903 24945 16696

usando a *chave privada* (e,n). ■

3.2.3 Desencriptação

De posse da *chave privada* (d,n) e o alfabeto escolhido (Figura 03):

(D_1) Inverter o processo descrito em (E_2), isto é, $m = c^d \ mod(n)$.

(D_2) Repetir o item (D_1), em todas as letras codificadas.

(D_3) De posse dos números decodificados, retorna-se ao alfabeto escolhido em (G_4) e completa-se a decodificação.

Exemplo 03: Decodificando a mensagem cifrada ***18783 07881 25044 03903 24945 16696*** obtida no Exemplo 02.

De posse da chave privada $(d,n) = (80.983, 40.981)$ obtida no Exemplo 01 e aplicando (D_1), ou seja:

$$c^d \ mod(n) \ \equiv \ m,$$

para $c = 18873$, aplicando o mesmo algoritmo utilizado no Exemplo 02, tem-se:

$$18783^{80983} mod(40981) \equiv 24$$

Repetindo o processo para $c = 07881$, tem-se:

$$07881^{80983} mod(40981) \equiv 26$$

Prosseguindo para as demais letras:

$$25044^{80983} mod(40981) \equiv 18$$
$$03903^{80983} mod(40981) \equiv 21$$
$$24945^{80983} mod(40981) \equiv 23$$
$$16696^{80983} mod(40981) \equiv 27$$

Temos a decifragem: 24 *26 18 21 23 27***.** Que, retornando ao alfabeto escolhido, obtêm-se:

P	**R**	**I**	**M**	**O**	**S**
24	*26*	*18*	*21*	*23*	*27*

concluindo o processo. ■

3.2.4 Interceptação

Numa interceptação, a desencriptação pode ser efetuada de diversas formas (força bruta, fatoração, temporização ou análise estatística de um texto cifrado) (Stallings, 2014). Aqui simularemos a decodificação da mensagem através de um método matemático em que se busca uma forma de usar a *chave pública* para obter a *chave privada* por meio de *fatoração* e conhecimentos de *aritmética modular*.

De posse da *chave pública* (e,n), um possível roteiro para encontrar a *chave* privada (d,n) é descrito a seguir:

(I_1) Encontrando p e q (fatorando n)

Necessita-se encontrar dois números primos, p e q, tais que $p \cdot q = n$. Como é bem desafiador obtê-los, uma forma seria através do teste probabilístico Miller Rabin (Stallings, 2014). Já para primos não muito grandes, uma das maneiras mais básicas é através de uma lista de primos ou do *Crivo de Erastóstenes* (Coutinho, 2015).

(I_2) Descobrindo o d

Sabe-se que $(e \cdot d)\ mod\varphi(n) = 1$, que remete à *equação diofantina*:

$$\varphi(n) \cdot y + e \cdot d = 1, \text{ onde } y\ \epsilon\ \mathbb{Z} \text{ e } \varphi(n) = (p-1) \cdot (q-1)$$

(I_3) Descobrindo o alfabeto.

Mesmo de posse da *chave privada* e decodificando os números correlacionados com as letras do alfabeto, é preciso saber a quais letras esses números estão associados. Em tal situação, é comum o trabalho estatístico (Souza e Pires, 2018; Pellegrini 2019), no qual recorre-se a uma tabela de frequência de uso de cada letra do alfabeto numa determinada língua.

(I_4) Decodificando.

De posse dos números d e n, ou seja, da *chave privada*, segue-se os passos de desencriptação descritos na seção 3.2.3

Exemplo 04: Suponha que deseja-se decodificar a mensagem

18783 07881 25044 03903 24945 16696

conforme o que foi feito no Exemplo 02, mas sem o conhecimento de p e q, supondo ainda que se conhece a *chave pública*

$$(e, n) = (40.491, 40.981)$$

De acordo com (I_1), é necessário fatorar $n = 40.981$.
Sem perca de generalidade, suponha que $p < q$. Observe que:

$$p < q \Rightarrow p^2 < p \cdot q \Rightarrow p < \sqrt{p \cdot q} \Rightarrow p < \sqrt{n}$$

Do mesmo modo,

$$p < q \Rightarrow p \cdot q < q^2 \Rightarrow \sqrt{p \cdot q} < q \Rightarrow \sqrt{n} < q$$

Ou seja,

$$p < \sqrt{n} < q$$

Logo, um dos primos procurados é menor que $\sqrt{n}$, o que reduz o intervalo de números inteiros no qual se deve buscar tal primo.
Segundo (C_1), p e q devem diferir em alguns dígitos e $\sqrt{n} < 203$. Usando o *Crivo de Erastóstenes* e os *critérios de divisibilidade*, os primos com 3 dígitos e candidatos a p são:

$$p = \{101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199\}$$

Testando cada um deles, de modo que se tenha $\frac{n}{p}$ inteiro, para $p = 107$, obtém-se:

$$\frac{n}{p} = \frac{40981}{107} = 383$$

Ou seja:

$$p = 107$$
$$q = 383$$

Como o $mdc(e, \varphi(n)) = 1$, para $e = 40.491$ e $\varphi(n) = 40.492$, e os valores de p e q são conhecidos, encontra-se d, de acordo com (I_2), resolvendo-se a *equação diofantina*:

$$e \cdot d + y \cdot \varphi(n) = 1$$

Isto é,

$$40.491 \cdot d + 40.492 \cdot y = 1$$

Logo

$$1 = 40.492 - 40.491 \cdot 1 \Rightarrow$$
$$1 = 40.491 \cdot (-1) + 40.492 \cdot 1$$

tem-se como solução particular

$$d = -1$$
$$y = 1$$

sendo assim, chega-se a solução geral

$$d = 40.492 \cdot k - 1, \text{com } k \in \mathbb{Z}$$

escolhendo $k = 2$, obtém-se

$$d = 40.492 \cdot 2 - 1$$
$$= 80.984 - 1$$
$$= 80.983$$

Logo, a chave privada é $(d, n) = (80.983, 40.981)$. ■

3.3 APLICAÇÕES

Devido à complexidade de implementação da técnica, o uso do RSA é mais comum em mensagens curtas, e-mails, comércio virtual ou em assinaturas

digitais, sendo portanto, menos recomendado para mensagens mais longas. O seu uso no comércio virtual ajuda a manter a segurança de dados nas transações com cartões de crédito (Stallings, 2014).

À medida que a tecnologia avança, os esforços computacionais de força bruta para quebrar uma chave se reduzem, mesmo assim o RSA mantém-se forte quando executado conforme as regras básicas de criação de chaves sugeridas pelos seus autores. Em parte, isso se deve à capacidade do RSA em gerar chaves cada vez maiores, pois se uma chave de 512 bits estiver obsoleta, é possível trocá-la por uma maior, como a de 1024 bits que, por sua vez, pode ser trocada por outra ainda maior. O problema é que a complexidade do processamento também aumenta, causando mais lentidão no sistema, o que nem sempre é proporcional a evolução computacional das máquinas (Stallings, 2014).

Segundo Valenta et al. (2015), usando-se cerca de 2.770 núcleos[5], uma chave de 512 bits requer menos de quatro horas para ser fatorada. Já uma chave 829 bits, chamada de RSA-250 que foi fatorada em 2020, levou aproximadamente sete dias usando 2.700 núcleos e, embora a quebra tenha representado um avanço na velocidade de fatoração, ainda não representa perigo às chaves existentes, uma vez que não são tão grandes quanto uma de 2048 bits que já é utilizada atualmente (Zimmermann, 2020).

Uma curiosidade interessante seria descobrir o tempo que o Frontier, o computador mais poderoso do mundo atualmente (Oak, 2020), levaria para quebrar uma chave RSA de 1024 bits. Como não foram encontrados registros de uma atuação do Frontier em alguma chave RSA, é possível estimar, grosseiramente, com base em sua quantidade de núcleos, o tempo que levaria para quebrar tal chave. Com a capacidade de aproximadamente 22.836 núcleos, estima-se que este computador exigiria pouco menos de 57 minutos em ter sucesso nesse intento. Contudo, a dificuldade de fatoração não é linear sendo de ordem exponencial, tanto é que a fatoração de uma chave de 1024 bits ainda não foi alcançada (Oak, 2020).

Uma forte ameaça mesmo tomando-se todos os cuidados descritos anteriormente, poderia vir com a computação quântica através do algoritmo de Shor (Cassinleo; Gómez, 2012).

[5] Referente a quantidade de núcleos de processamento em uma CPU. Um ano de núcleo é o equivalente a usar um núcleo de CPU continuamente por um ano inteiro.

Ainda nesta direção, existe um problema em aberto na matemática pura, conhecido como a *Hipótese de Riemann*, em torno da qual há um temor de que, quando resolvido, a solução traga consigo algum algoritmo que possibilite a fatoração de maneira simples (Sautoy, 2008).

Ou seja, enquanto computadores do porte de um Frontier não sejam de fácil acesso e a computação quântica não se torna realidade, a *criptografia* RSA continua sendo um algoritmo seguro.

4 O JOGO E COMO EXPLORÁ-LO

Um dos problemas detectados na área de matemática, através de testes de sondagem e observações em sala de aula, está relacionado com as quatro operações básicas: (adição, subtração, multiplicação e divisão) quando aplicadas aos mais variados contextos, tendo-se aprofundado ainda mais, em um cenário pós pandemia.

Inserir um jogo online que, de alguma forma desperte o interesse do aluno e ainda sirva como exemplo prático explorando conceitos matemáticos que abranjam essas dificuldades, seja inovador e curioso, certamente se apresenta como uma boa opção de aprendizagem o jogo **RSA-CrypTa**.

Este jogo, que simula uma interceptação de mensagens por um hacker, exige por parte do jogador conhecimentos matemáticos sobre *números primos, mmc, mdc, divisão, multiplicação, adição e subtração de números inteiros*, ainda na primeira fase. Já na segunda fase, a exigência é sobre a resolução de uma *equação diofantina* que, assim como na fase anterior, também requer habilidades nas operações aritméticas para a sua resolução. Na terceira e última fase, o jogador é estimulado a pensar dedutivamente a fim de reconhecer padrões e utilizá-los em seu benefício. Dessa forma, é possível verificar tais conhecimentos de uma forma divertida, lúdica, curiosa e moderna, já que desperta o interesse do aluno na compreensão das mensagens hackeadas tendo o seu próprio celular como ferramenta de aprendizagem.

4.1 RSA-CRYPTA

O jogo, desenvolvido como parte deste trabalho, foi nomeado de **RSA-CryPta** e encontra-se disponível online, podendo ser acessado no endereço eletrônico:

https://www.docentes.univasf.edu.br/edson.araujo/rsa

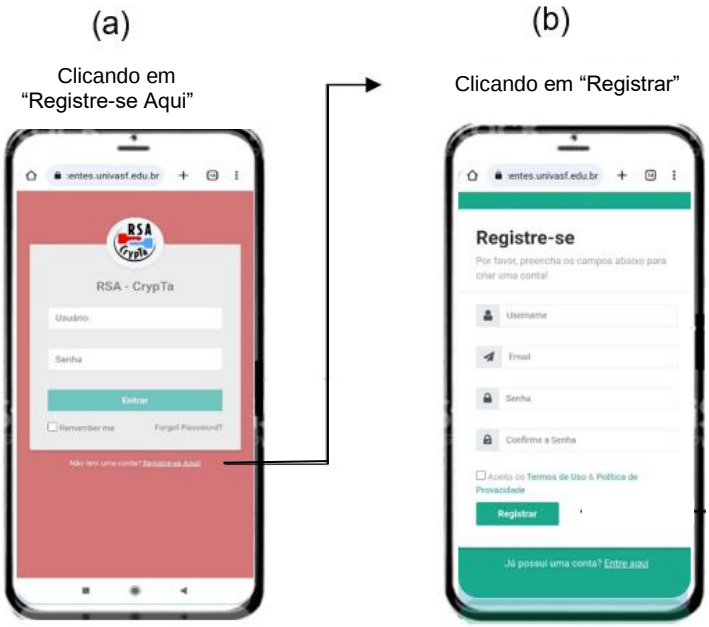
Foi adaptado para aparelhos celulares, muito embora também possa ser usado em computadores ou tablets através de quaisquer navegadores.

4.1.2 Entrando no Jogo

Apesar de ser possível acessar o **RSA-CryPta** tanto por computador como por celular, para melhor compreensão, toda a explicação do seu funcionamento se priorizará na versão celular, tendo em vista ser esta versão que foi utilizada com os estudantes, embora algumas menções de uso no computador também ocorram.

No primeiro acesso, o usuário deve se cadastrar (Figura 04b), sendo necessário para isto que sejam informados nome, e-mail e senha. Esta tela de registro pode ser acessada clicando em “Registre-se Aqui” que se encontra na tela inicial do aplicativo (Figura 04a)

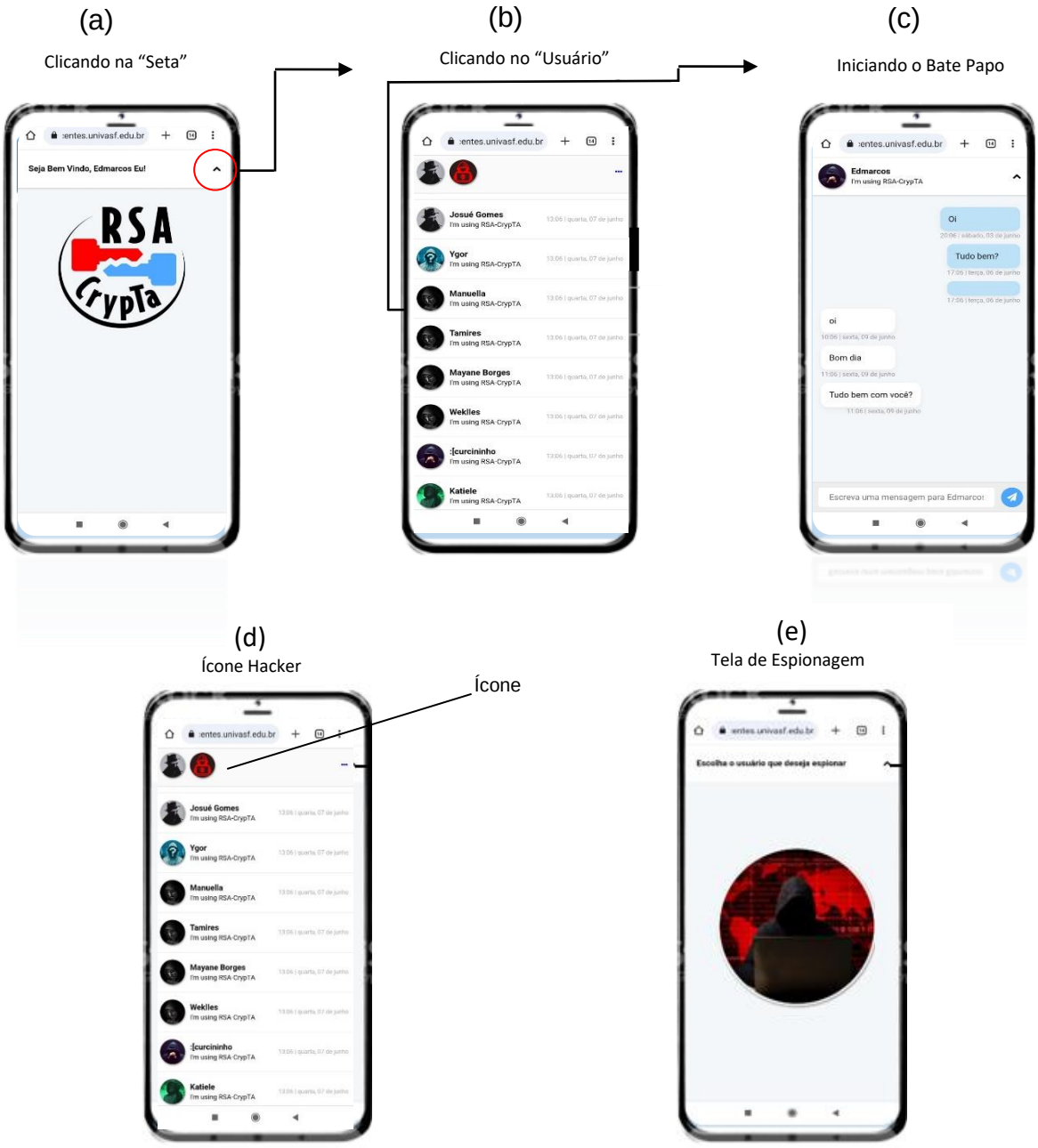
Figura 04: Tela inicial



Fonte: Os Autores.

Uma vez *efetuado* o registro, o aluno será redirecionado à tela inicial e realizará sua entrada clicando em “*Entrar”,* após colocar o nome de usuário e senha registrados e ao entrar, o usuário é direcionado para a tela de “*Boas Vindas”* (Figura 05a), onde o jogador, clicando na seta situada no canto superior direito, tem acesso a todos os usuários cadastrados (Figura 05b) com os quais pode conversar (Figura 05c) ou tentar espionar suas conversas (Figura 05d).

Figura 05: Entrando no jogo – Versão celular



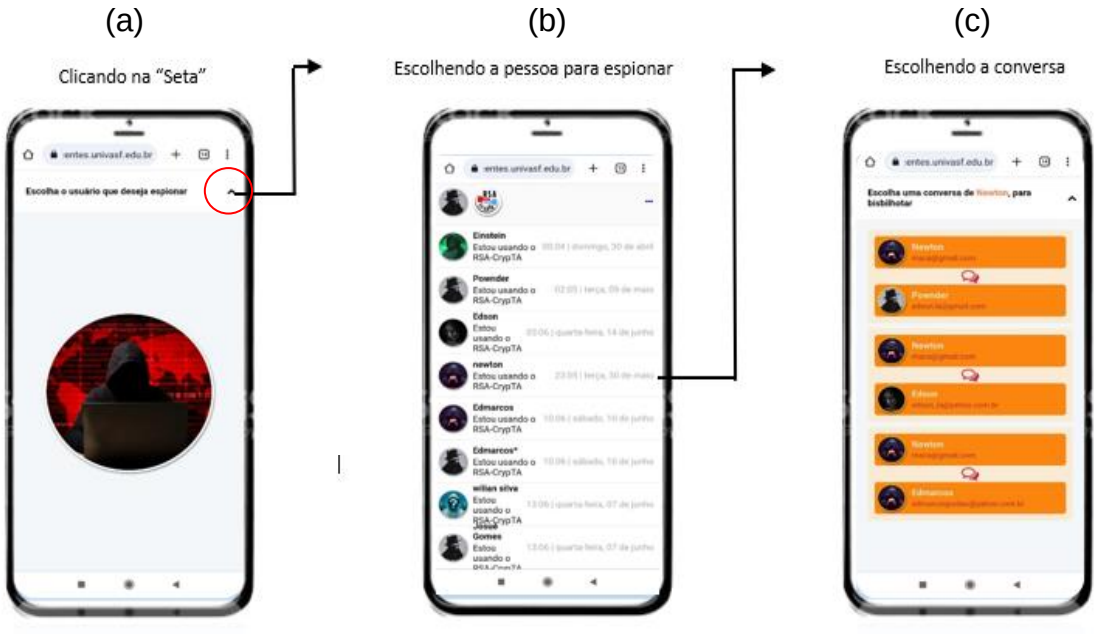
Fonte: Os Autores

4.1.3 Interceptando uma conversa

Para espionar uma conversa, o jogador deve clicar no *ícone hacker* situado no canto superior à esquerda (Figura 05d), que o direciona a "*Área Hacker*" (Figura 05e). Na seta localizada no canto superior à direita (Figura 06a), o usuário tem acesso a uma nova tela dando acesso a todos os usuários que já conversaram

no bate-papo do aplicativo e que podem ser alvo de sua interceptação (Figura 06b). Ao escolher o usuário que deseja espionar e clicar sobre o seu nome, o aplicativo exibe uma tela contendo todas as conversas que este usuário já realizou (Figura 06c).

Figura 06: Área hacker – Versão celular

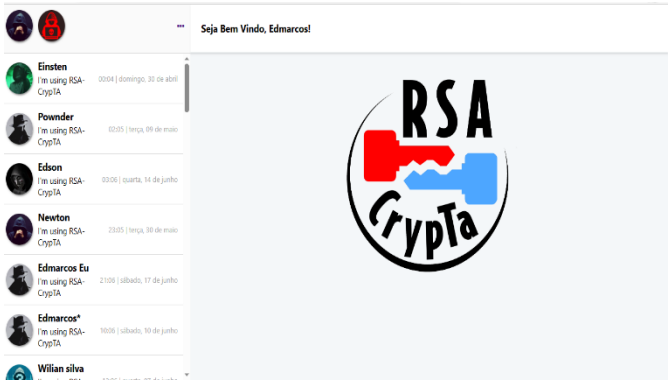


Fonte: Os Autores

Figura 07: Entrando no jogo – Versão computador

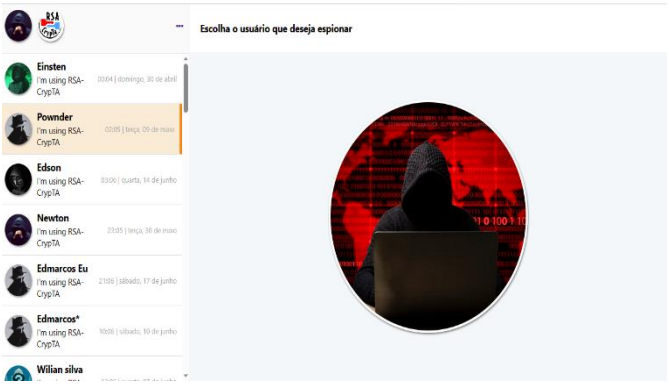
(a)

Tela de Boas-Vindas



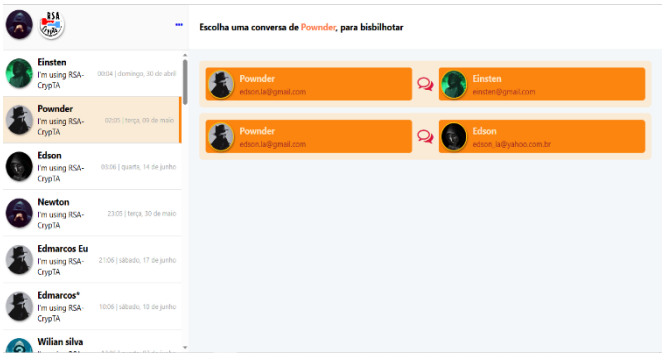
(b)

Tela de Espionagem



(c)

Escolha do Diálogo

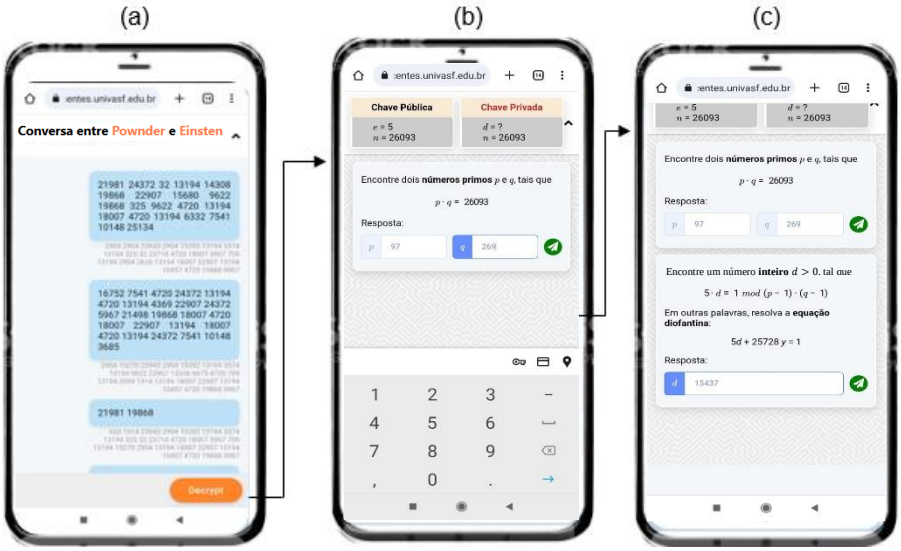


Fonte: Os Autores.

As Figuras 07a, 07b e 07c, exibem as versões em dispositivos de tela maior que um celular (tablet, notebook, computador e outros) das Figuras 06a, 06b e 06c, respectivamente.

Após a escolha do diálogo a bisbilhotar, o jogador será direcionado a uma tela com todo o conteúdo da mensagem *codificado* em RSA (Figura 08a).

Figura 08: Clicando em uma das mensagens – Versão celular



Fonte: Os Autores

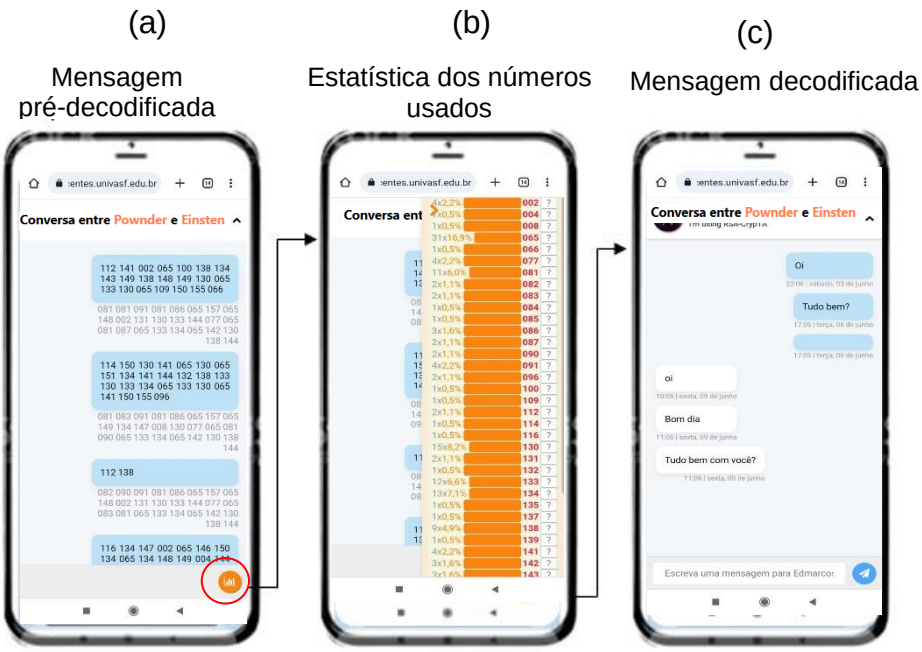
Clicando em "*Decrypt",* o jogador será direcionado a uma tela com as informações da *chave pública,* (e,n), chegando ao que vem a ser a **1ª Fase** do jogo (Figura 08b). O usuário é desafiado a encontrar dois números primos, p e q tais que $p \cdot q = n$. Ao inserir os valores de p e q corretamente, o ícone e, **azul** no lado direito da tela torna-se **verde**, indicando sucesso na tarefa.

Ao clicar no botão **verde**, o usuário tem acesso ao que vem a ser a **2ª Fase** do jogo (Figura 8c). Nesta etapa, o desafio consiste em descobrir o valor do expoente de desencriptação d, sendo necessário para isto resolver uma *equação diofantina* exposta em tela e montada a partir dos valores de p e q, descobertos anteriormente. Novamente, ao inserir o valor correto para d, o segundo botão azul no lado direito da tela ficará **verde**, indicando a correta resposta para o desafio e dando acesso à **Fase final** do jogo (Figura 09a).

Nessa etapa, o jogador encontrará a mensagem ainda codificada, porém, de uma forma mais simples (*Cifra de César*), necessitando ainda que o usuário

descubra o embaralhamento (deslocamento) feito no alfabeto padrão, podendo para isto, usar a estatística para descobrir cada letra (Figura 09b). Tal estatísitca é realizada a partir da conversa interceptada, contando quantas vezes cada caractere aparece. Pode ser acessado através do *ícone laranja* que encontra-se no canto inferiror direito da tela (Figura 09a).

Figura 09: Decifrando a mensagem – Versão celular

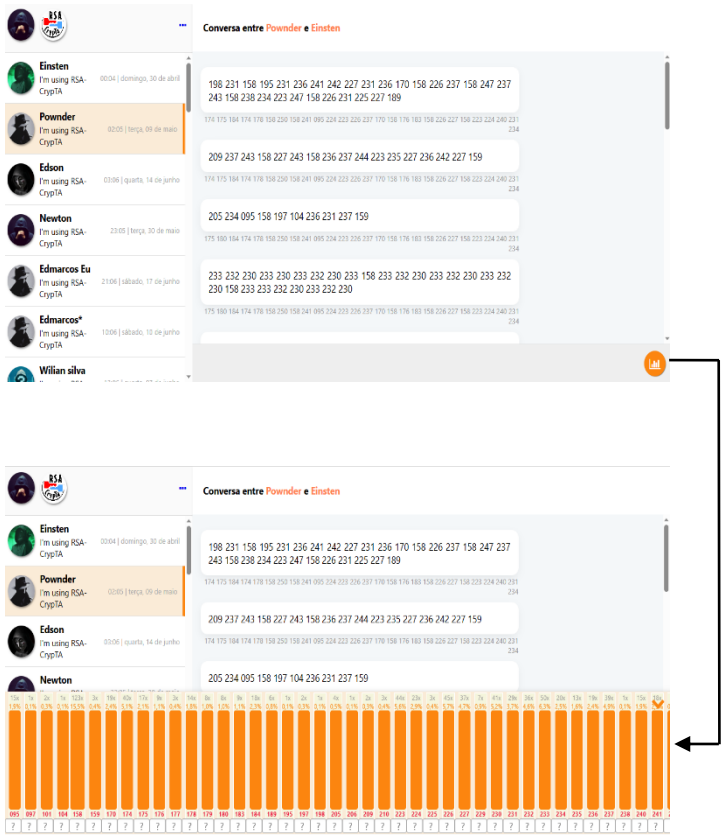


Fonte: Os Autores

Clicando no *ícone laranja*, a tela exibirá um levantamento completo a respeito da mensagem contendo a quantidade de vezes e o percentual que um determinado caractere (na verdade seu respectivo código numérico) foi usado na mensagem (Figura 09b). Para cada caractere, há uma caixa de entrada, situada ao lado de suas respectivas informações, no qual o usuário pode inserir a letra que entenda ser a resposta. Uma vez deduzida todas as letras, a mensagem, enfim, será revelada, como mostrado na Figura 09c.

Na versão para computador, a interface muda um pouco, como mostra a Figura 10, mas o processo dedutivo é exatamente o mesmo.

Figura 10: Decifrando a mensagem – Versão computador



Fonte: Os Autores

A dedução de cada um dos caracteres pode ser realizada através de padrões observados nas mensagens que são enviadas e recebidas em um diálogo do próprio usuário com outra pessoa (Figura 11) e que servem como pistas para inferir.

4.1.4 Explorando o jogo

Em cada uma das fases do jogo, desafios são propostos ao usuário e, para solucioná-los, alguns conceitos matemáticos são necessários. Nas subseções a seguir é exibido como tais conceitos podem ser explorados.

Fase 01: Encontrar p e q

Aqui, o professor terá possibilidades de explorar a fatoração, números primos, critérios de divisibilidade e até a criação do Crivo de Erastóstenes.

Esta fase pode ser bem desafiadora e demorada se o aluno não possuir uma boa estratégia de busca para p e q. Ao testar a divisão de n por todos os números entre 2 e n, tal tarefa se revelará muito demorada. Isso pode ser atenuado usando o *critério da raiz quadrada* mencionado no Exemplo 04, o que fará com o que a busca se reduza apenas aos números ímpares e primos menores que $\sqrt{p \cdot q}$ disponíveis no *Crivo de Erastóstenes* que eles mesmos devem construir.

Exemplo 05: Suponha $n = 26093$. Observe que:

$$\sqrt{n} = \sqrt{26093}$$

$$= 161{,}533278 \ldots$$

Ou seja, um dos primos que deseja-se encontrar é menor que 161. Elencando todas as possibilidades, chega-se ao conjunto:

$$S = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,$$
$$101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157\}$$

Efetuando a divisão de n pelos elementos de S, nota-se que 97 é um dos valores com divisão inteira. Procedendo agora com a divisão de n por 97, obtém-se 269. Deste modo, tem-se os números primos $p = 97$ e $q = 269$, tais que $p \cdot q = n$. ■

Uma observação que merece destaque nesta fase concerne aos alunos PcDs com paralisia cerebral nível I e com algum grau de retardo de raciocínio, pois essa fase do jogo permite explorar conteúdos matemáticos apropriados ao problema de saúde detectado. A exemplo disto, muitos desses alunos têm dificuldade na compreensão da sequência de contagem de 0 a 100 ou 0 a 1000, em números pares e ímpares, soma, subtração, multiplicação e divisão. Em relação às operações básicas é possível superar tal dificuldade com o uso da calculadora. O nível de dificuldade destas operações no jogo é alto para eles, no entanto não impede que sejam bem-sucedidos, amparando-se uma vez mais em aparatos tecnológicos. Seguindo adiante, ao usarem o critério da raiz quadrada para encontrarem p e q, exige o manuseio correto da calculadora (alguns têm dificuldade motora nas mãos e até na fala) e a exploração das sequências adequadas dos números ímpares. Além

disso, é uma ótima oportunidade para inseri-los juntos aos demais alunos nessa mesma fase do jogo sem adaptações adicionais na atividade que difeririam a deles das dos demais ajudando-os a sentirem mais acolhidos pela turma a que pertencem.

Considerando que ensino tradicional se mostrou inadequado para esses alunos, o celular, quando utilizado de forma adequada, oferece a possibilidade de maior concentração, permitindo que avancem nos conteúdos de maneira mais curiosa, lúdica e motivadora. Uma forma de alcançar esse objetivo é através do jogo **RSA-CrypTa**.

Fase 02: Encontrar d resolvendo a equação diofantina

Nesta fase, o *mdc*, o *Teorema de Euclides* e a *equação da reta* se apresentam como conteúdos que podem ser explorados pelo professor. É uma fase mais robusta, tendo em vista que exige encontrar a equação da reta com coeficientes e raízes inteiras, uma vez confirmada a sua existência através do uso do mdc. Mais uma vez a divisão é usada com ênfase na sua resolução manual, aparatos tecnológicos, com a finalidade da detecção do resto.

Exemplo 06: Considere o número $n = 26093$, $p = 97, q = 269$ e $e = 5$ (*chave pública*). Chega-se a *equação diofantina*:

$$e \cdot d + \varphi(n) \cdot y = 1 \Leftrightarrow$$
$$5d + 25728y = 1$$

O *Teorema de Euclides* é necessário. O que faz com o que aluno obrigatoriamente use as quatro operações básicas em conexão aos conhecimentos sobre números inteiros e racionais, uma vez que números “quebrados”, tipo $1{,}2$ ou $3{,}12$ não são permitidos.

Note que o $mdc(5d, 25728) = 1$, implica em $5d \equiv 1\ mod(25728)$, usando o *Teorema de Euclides*, percebe-se que:

$$3 = 25728 - 5 \cdot 5145 \quad (1)$$
$$2 = 5 - 3 \cdot 1 \quad (2)$$
$$1 = 3 - 2 \cdot 1 \quad (3)$$

Por (2) em (3):

$$1 = 3 - (5 - 3 \cdot 1) \cdot 1 \Rightarrow$$
$$1 = -5 + 3 + 3 \cdot 1 \Rightarrow$$
$$1 = -5 + 3 \cdot 2 \qquad (4)$$

Por (1) em (4)

$$1 = -5 + (25728 - 5 \cdot 5145) \cdot 2 \Rightarrow$$
$$1 = -5 + 2 \cdot 25728 - 2 \cdot 5 \cdot 5145 \Rightarrow$$
$$1 = -5 + 2 \cdot 25728 - 5 \cdot 10290 \Rightarrow$$
$$1 = -5 \cdot 10291 + 25728 \cdot 2 \Rightarrow$$
$$1 = 5 \cdot (-10291) + 25728 \cdot 2$$

Tem-se como solução particular,

$$d = -10291$$
$$y = 2$$

e solução geral

$$d = d_0 + b \cdot t$$
$$y = y_0 - a \cdot t$$

Como é necessário um valor inteiro positivo para d, através da solução geral, tem-se, para $t = 1$:

$$d = -10291 + 25728 \cdot 1$$
$$= 15437 \qquad \blacksquare$$

Um paralelo com a *equação da reta* e *função do primeiro grau* podem ser explorados, inclusive com o uso do Geogebra, a critério do professor, para mostrar o comportamento gráfico da função oriundo da *equação diofantina* para valores inteiros.

É uma fase com muitas “continhas” em que o aluno precisará usar papel e caneta para a sua resolução.

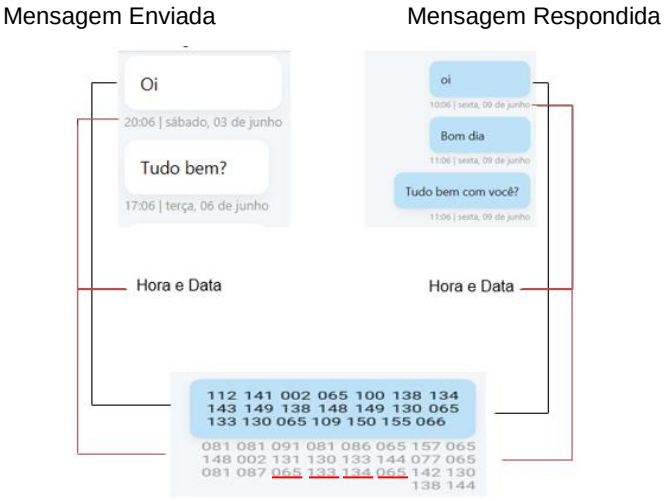
Fase 03: Decifrar a Codificação

Com o valor de d encontrado anteriormente, finalmente chega-se à Fase 03. Nesta etapa são adicionados mais elementos interdisciplinares que conectam os assuntos e fases passadas com o mundo real atrelado ao virtual. O aluno deverá mostrar conhecimento da forma culta e coloquial da língua portuguesa e uma capacidade relevante de observação e pensamento dedutivo com base nas estatísticas apresentadas na fase.

Inserindo nas caixas do leque estatístico o caractere que cada código numérico representa, esta última fase do jogo traz a possibilidade de extrair do aluno o pensamento dedutivo através de inferências que podem ser realizadas com o auxílio da estatística utilizada no jogo.

Uma vez deduzidas todas as letras, ou a maioria delas, já é possível ler ou compreender o conteúdo da mensagem criptografada agora, (descriptografada).

Figura 11: Entendendo as pistas – Versão celular ou computador

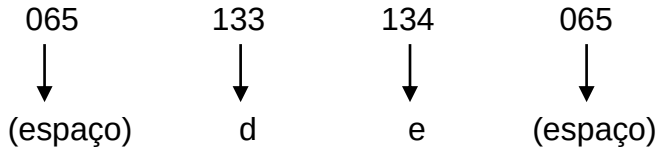


Fonte: Os Autores

Pela Figura 11, é possível observar uma mensagem em andamento que, quando espionada por um jogador (Figura 09a), estará ainda codificada com a parte dentro dos balões (azul e branco) correspondente às mensagens trocadas, e a parte abaixo destes, à hora e data em que foram emitidas. O registro da data e hora que uma mensagem foi emitida ou recebida, obedece ao seguinte padrão:

hh:mm | *dia, xx, de xxxxx*

Observando a lista de números apresentadas na Figura 09, parte cinza, e ao associar a hora e data emitidos (Figura 11), é possível deduzir alguns caracteres. Por exemplo,a penúltima linha da parte cinza da Figura 11, com a sequência 065 133 134 065, correspondem a: (espaço) **d e** (espaço), ou seja:



Uma vez conhecidas as letras minúsculas “d” e “e”, o jogador poderá deduzir que todas as outras letras estão em sequência, conforme a *Cifra de César*. Por exemplo, se a letra “f” corresponde 135, o “g” corresponde a 136, o “e” será o 134, e assim por diante. Em busca de mais **pistas** é possível deduzir também caracteres especiais como “:”, “,” ou mesmo “|” presentes nos horários e datas que acompanham cada mensagem enviada e recebida. Mais um pouco de investigação e se consegue obter também as letras maiúsculas que, como as minúsculas, obedecem a mesma lógica das maiúsculas, isto é, se o jogador deduzir que a letra “C” maiúscula corresponde ao número 239, então as letras D, E e F serão, respectivamente, 240, 241 e 242, ao passo que as letras A e B serão 237 e 238.

4.2 METODOLOGIA

De natureza *qualitativa* com finalidade de aplicação, esta pesquisa classifica-se como *experimental*, uma vez que avalia um grupo específico de alunos: dois primeiros anos do *ensino médio* (**Turma A** com 31 alunos e **Turma B** com 35 alunos) (Lakatos; Marconi, 2003). A **Turma B** foi submetida a testes e experimentações que visam avaliar o seu aprendizado e curiosidade matemática tendo como recurso didático-pedagógico o uso de um jogo online, e a **Turma A** recebeu o mesmo conteúdo, porém tendo uma abordagem tradicional.

Ambas as turmas foram pré-avaliadas (Atividade de Sondagem, Apêndice C) no início do primeiro trimestre e após o término da primeira unidade[6] do ano

[6] No estado da Bahia, aluno é avaliado em três unidades de 10 pontos cada uma, somando ao total 30 pontos finais. O estudante deve tirar, até o fim do período letivo, pelo menos 15 pontos totais ou, 5 pontos em cada unidade

letivo, tendo seus desempenhos comparados a partir dos resultados, decidiu-se em qual delas aplicar-se-ia o jogo **RSA-CrypTa**. Esta avaliação diagnóstica teve como conteúdo as *operações aritméticas básicas, equações e função do primeiro grau*, por se entender ser o suficiente para a escolha de qual turma seria aplicado o jogo. Após a avaliação e verificada a dificuldade de cada turma, constatou-se que ambas não estavam com bom desempenho, sendo a **Turma B** inferior a **Turma A**. Foi a partir desse ponto que houve a escolha da **Turma A** para se trabalhar tradicionalmente e a **Turma B** para a intervenção com o jogo **RSA-CrypTa**.

Na Turma B, foi aplicada uma sequência didática (Apêndice B) com base no jogo. Ao término de todo o processo foi aplicado um *Questionário Qualitativo sobre* a percepção dos alunos quanto ao aplicativo (Apêndice D). Na **Turma A** foi explorado o mesmo conteúdo, porém de modo tradicional utilizando-se apenas o quadro branco, pincel, caderno, lápis, atividades escritas e observações, mas sem o uso do jogo ou qualquer meio digital.

Para efeito de comparação entre a introdução proposta neste trabalho e a abordagem tradicional, foi realizado uma avaliação comparativa, composta por duas atividades, 01 e 02 (Apêndice C) cujos resultados são expostos no capítulo a seguir.

Realizada no ano de 2023, segundo trimestre, a turma escolhida para a aplicação do jogo **(Turma B)** é composta por 35 alunos entre 15 e 17 anos, na *Escola Estadual de Tempo Integral Manoel Novaes,* Curaçá-BA. Dois alunos com paralisia cerebral de grau I e algum retardo mental também participaram da pesquisa. Esses alunos são classificados como "Pessoas com Deficiência" e sua participação permitirá observar como o jogo pode contribuir para o aprendizado deles.

4.3 SEQUÊNCIA DIDÁTICA

O **RSA-CrypTa** foi usado como recurso didático na Turma B, e usado para a construção de uma sequência didática abordando números primos, fatoração, mmc, mdc e equação do primeiro grau consistindo em um total de 14 aulas de 50 min cada (Apêndice B). O mesmo conteúdo, na mesma quantidade de aulas também foi abordado na Turma A, porém totalmente no modo tradicional.

Para a Turma B, a sequência faz previsões de 02 aulas para registro dos alunos no jogo ***RSA-CrypTa*** e a apresentação do que é criptografia e o sistema

RSA, 02 aulas sobre *equações do primeiro grau*, 02 aulas sobre *números primos* e *fatoração*, 01 aula sobre *raiz quadrada*, 04 aulas sobre *equação da reta* e *equação diofantina* e, por fim, 03 aulas de aplicação do jogo, totalizando 14 aulas.

5 RESULTADOS E DISCUSSÕES

A avaliação diagnóstica das turmas se deu através da comparação em percentual de acertos na *Atividade de Sondagem* (Apêndice C), aplicado no início do período letivo. Os resultados encontram-se na Tabela 01:

Tabela 01: Comparativo de desempenho por acerto das turmas A e B

	Turma A	Turma B
Teste de sondagem	76%	48%

Fonte: Dados da pesquisa

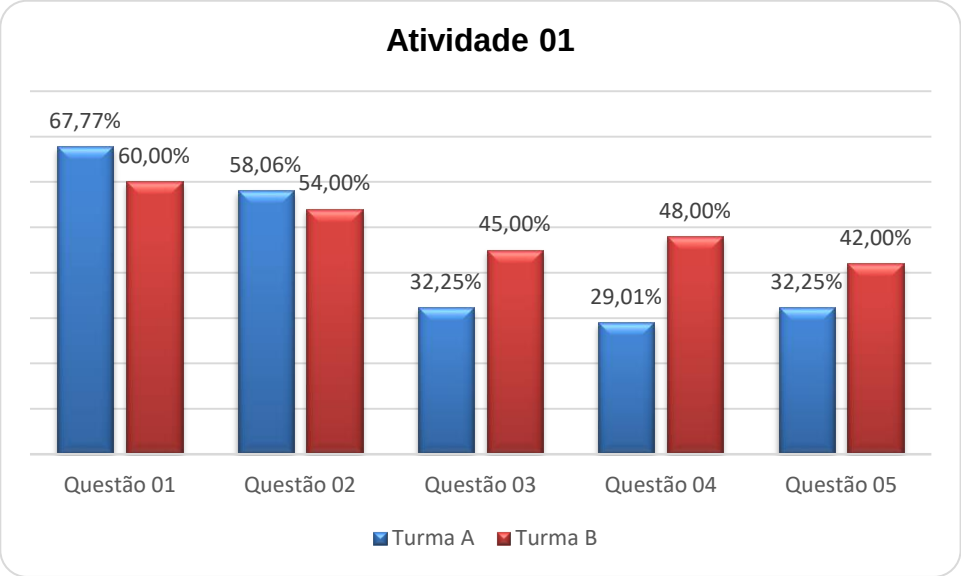
É importante salientar que, o conteúdo apresentado em ambas as turmas consistia em uma revisão sobre as operações básicas com números reais com ênfase aos números inteiros, culminando com função do primeiro grau.

No se que refere à sequência didática, toda ela foi criada segundo as dificuldades encontradas no teste de sondagem e no perfil da turma, sendo plenamente aplicada e executada conforme o planejado com algumas pequenas variações, mas nada que comprometesse o planejado. Não estava previsto, por exemplo, que os alunos acessassem o **modo espião** do jogo antes do professor explicar e autorizar, no entanto o fizeram, o que resultou em uma grande comoção e curiosidade por parte deles em descobrir o porquê das mensagens acessadas estarem todas em forma de números e o que poderiam fazer para a entenderem.

5.1 AVALIAÇÃO COMPARATIVA

Ambas as turmas, no decorrer das aulas 01 a 14, resolveram duas atividades escritas, chamadas de *Atividade 01* e *Atividade 02*, com o intuito de avaliar a absorção dos conceitos. O Gráfico 01, aponta os resultados, em percentual de acertos na *Atividade 01*.

Gráfico 01: Desempenho - Atividade 01



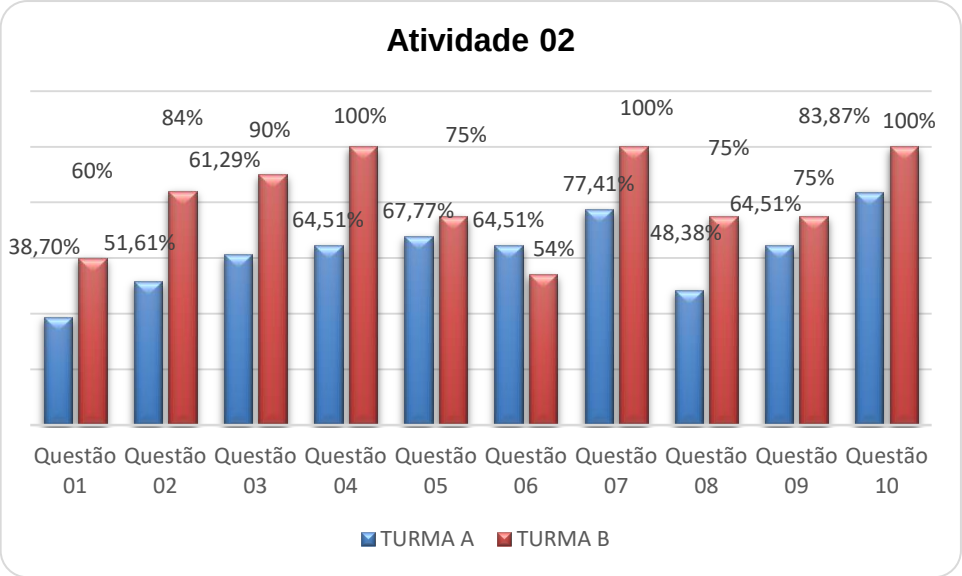
Fonte: Dados da pesquisa

Na **Turma B**, as questões 01 a 02, sobre *mmc*, obteve um índice de acertos entre 54% e 60%, ao passo que a **Turma A**, nas mesmas questões, obteve um resultado superior entre 58% e 68%. Já as questões 03 a 05, sobre *mdc*, a **Turma B** ficou entre 42% e 48%, e a **Turma A** ficou mais abaixo, entre 29% e 32%. No geral, nessa atividade, a **Turma B** alcançou uma média de 49,8% e a **Turma A** uma média de 43,87%.

Na *Atividade 02*, mais longa que a *Atividade 01*, em média 78% dos alunos da **Turma B** acertaram a questões 01 a 03 (sobre equação do primeiro grau), ao passo que a **Turma A** obteve uma média de 50,53%. As questões 04 a 06 sobre fatoração, o desempenho médio da **Turma B** foi pouco mais de 76% com uma pequena queda da questão 06. Já a **Turma A**, teve assertivas de 65,59%. As questões 07 a 10, sobre *mmc*, *mdc* e números primos, o acerto médio foi pouco acima de 87,5% pela **Turma B** e de 68,54% pela **Turma A**.

No geral, a **Turma B** apresentou uma média de 81,3% nas 10 questões da Atividade 02, e a **Turma A** uma média de 62,25%. Já as duas atividades juntas apresentaram uma média de 65,55% pela **Turma B** e de 53% pela **Turma A**.

Gráfico 02: Desempenho - Atividade 02



Fonte: Dados da pesquisa

5.2 PERCEPÇÃO SOBRE O JOGO

Sobre o desempenho da **Turma B** usando o jogo online **RSA-CrypTa**, do quantitativo total de 35 dos alunos, 27 possuíam celular e os oito restantes acompanharam a o jogo sentando-se juntos com outros colegas em duplas. Nessa atividade, em toda sua primeira fase, os dois alunos especiais foram auxiliados pela sua cuidadora disponibilizada pelo NTE-10 (Núcleo Territorial de Educação 10 do estado da Bahia).

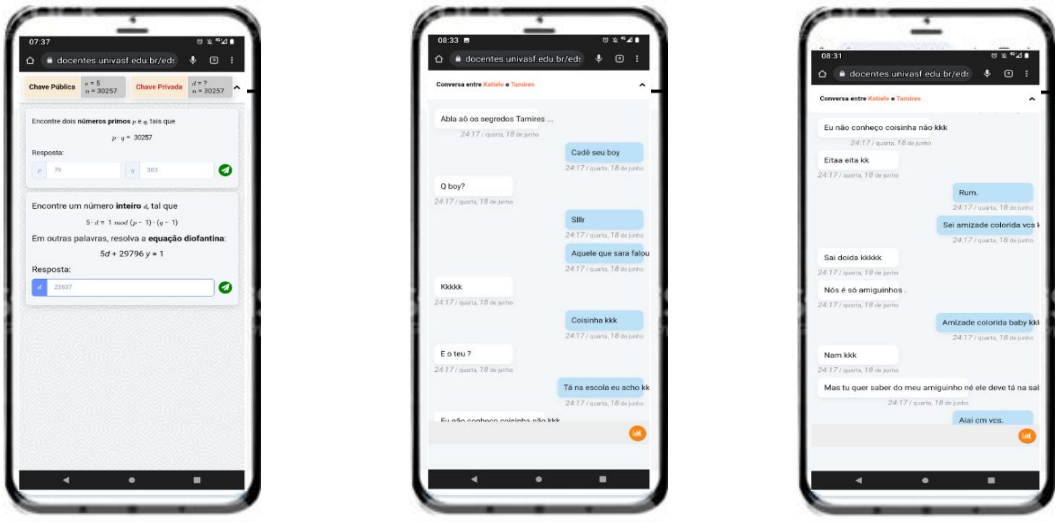
Na **Fase 01**, todos os 35 alunos completaram a tarefa, sendo que 33 desses o fizeram em até 05 minutos de jogo, ao passo que dois deles, os alunos especiais, gastaram entre 07 e 10 minutos para realizarem a mesma tarefa. Na **fase seguinte**, dos 33 jogadores (os dois alunos PcDs não conseguem ir adiante), 25 conseguiram a realizar no tempo previsto, ficando os demais sob a orientação do professor por mais 30min. A **Fase 03** foi completada com sucesso e a tempo por 20 alunos.

Em menos de 24 horas, de forma remota, todos os 33 alunos conseguiram completar as três fases com 20 deles no tempo correto e 13 fora do tempo. A Figura 12 mostra mensagens decodificadas por um desses alunos.

Infelizmente os dois alunos especiais ainda não sabem ler adequadamente, o que inviabilizou as outras fases. Avaliando os resultados sem

eles, 60,6% completaram todas as fases com sucesso no tempo determinado e 100% da turma conseguiu completar o jogo em até 24 horas.

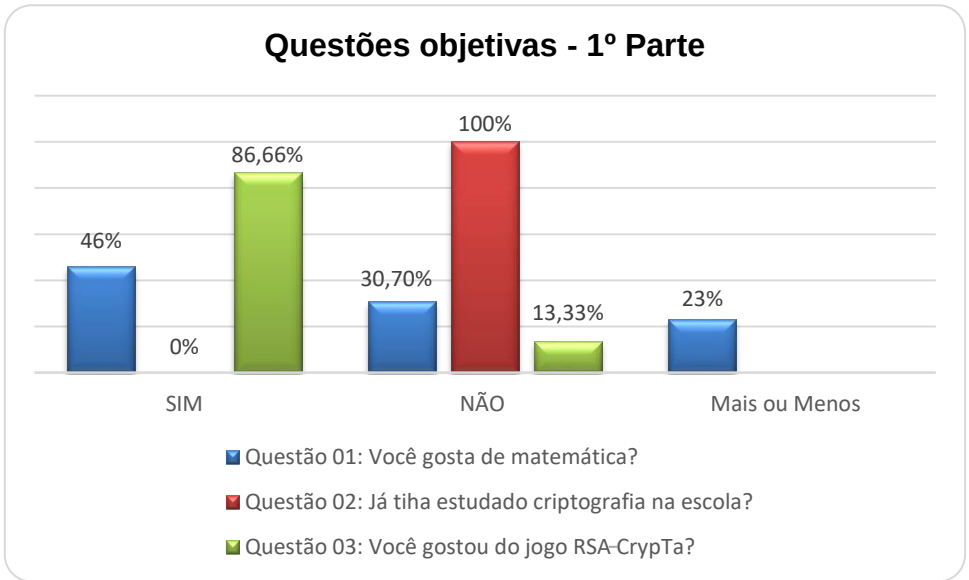
Figura 12: Invasão concluída com sucesso



Fonte: Os Autores

No questionário sobre a percepção do aluno da Turma B sobre o jogo (APÊNDICE D), foram feitas 08 perguntas das quais cinco delas são objetivas e as outras três dissertativas. O Gráfico 03 aponta as respostas de três dessas perguntas objetivas.

Gráfico 03: Respostas - Questões objetivas (1, 2 e 3)



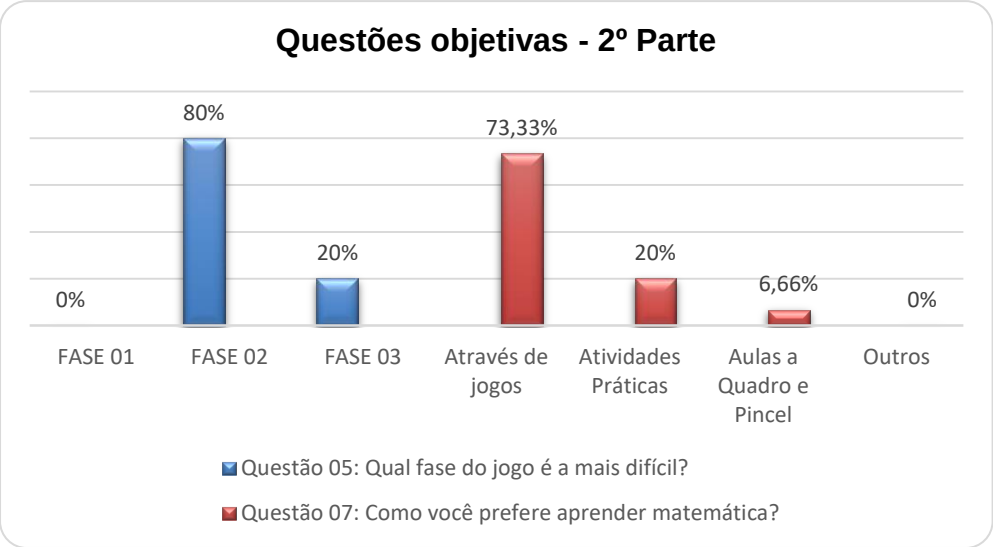
Fonte: Dados da pesquisa

Cerca de 46% dos alunos se dizem gostar de matemática, 30,7% não gostam e 13,33% a acham mais ou menos. O interessante nesse ponto é o número de alunos que se dizem gostar de matemática ser maior do que o número dos que não gostam.

Nenhum dos alunos tinha estudado criptografia antes na escola e 86,66% deles gostaram do jogo **RSA-CrypTa** com cerca de 13% que não gostaram. Perguntados sobre o porquê de não gostarem do jogo, 53% responderam que estava difícil e o restante não soube opinar.

O Gráfico 04 exibe as duas outras questões objetivas e seus resultados.

Gráfico 04: Respostas - Questões objetivas (05 e 07)



Fonte: Dados da pesquisa

Vê-se que claramente que a **Fase 02** foi considerada a mais difícil com 80%. Quando perguntados do motivo, responderam que era a fase que tinha mais “contas” a se fazer. O restante achou a **Fase 03** mais difícil e, segundo eles, faltava-lhes paciência para decifrar os códigos e os associar às letras do alfabeto.

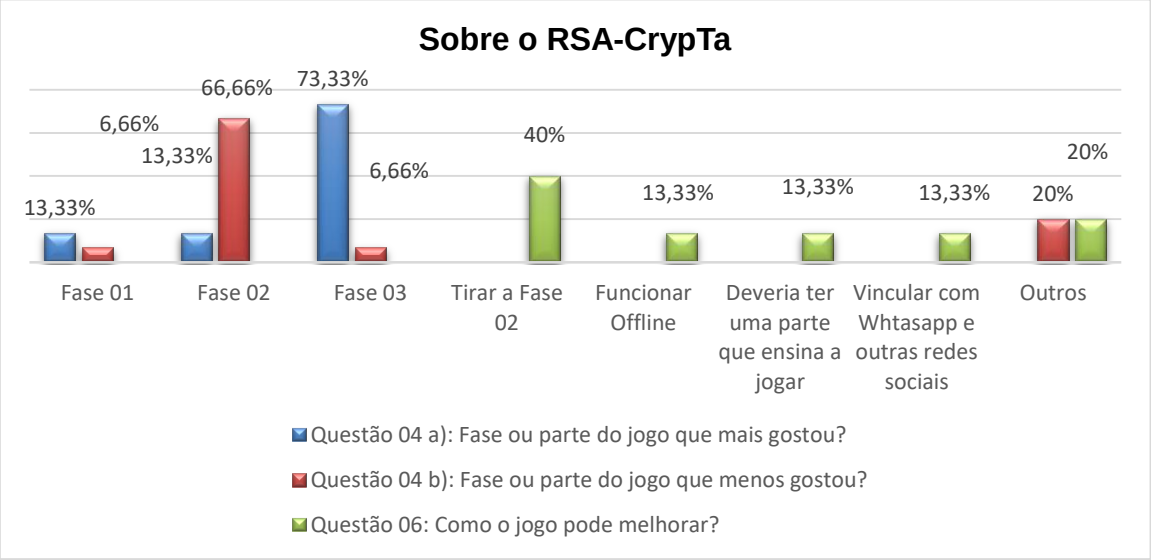
Já quando perguntados como preferiam aprender matemática, mais de 93% desejam aulas práticas ou com jogos, com cerca de 6% preferindo o método tradicional. Nas questões dissertativas, as respostas foram variadas.

Quando perguntados sobre o jogo em específico de que parte ou fase mais e menos gostaram (Gráfico 05), 73,33% optaram para a **Fase 03**, e as **Fases 01 e 02** ficaram empatadas com 13,33% cada. Já a fase ou parte do jogo que menos gostaram, 66,66% disseram que é a **Fase 02** e com 6,66% cada uma, ficaram

empatadas as **Fases 01 e 02**. Os 20% restantes optaram por outras partes do jogo que não gostaram, como não funcionar offline. Foi relatado também que a **Fase 03** era a mais aguardada, pois estavam curiosos em saber o conteúdo das mensagens encriptadas.

A próxima pergunta foi justamente como o jogo poderia melhorar e 40% afirmaram que seria melhor tirar a **Fase 02**, 13,33% disseram que o jogo deveria funcionar offline e mais outros 13,33% disseram que deveria haver alguma parte do jogo que os ensinassem a jogar. É curioso como uma parte relevante dos alunos, 13,33%, manifestaram interesse em hackear redes sociais reais como o Whatsapp e Instagram, pois acham que o jogo ficaria bem melhor se fosse atrelado a essas redes sociais. Aqueles que tirariam a **Fase 01 e 03**, os que disseram que "o jogo está bom assim mesmo" ou que "não tirariam nada" somam juntos cerca de 20%.

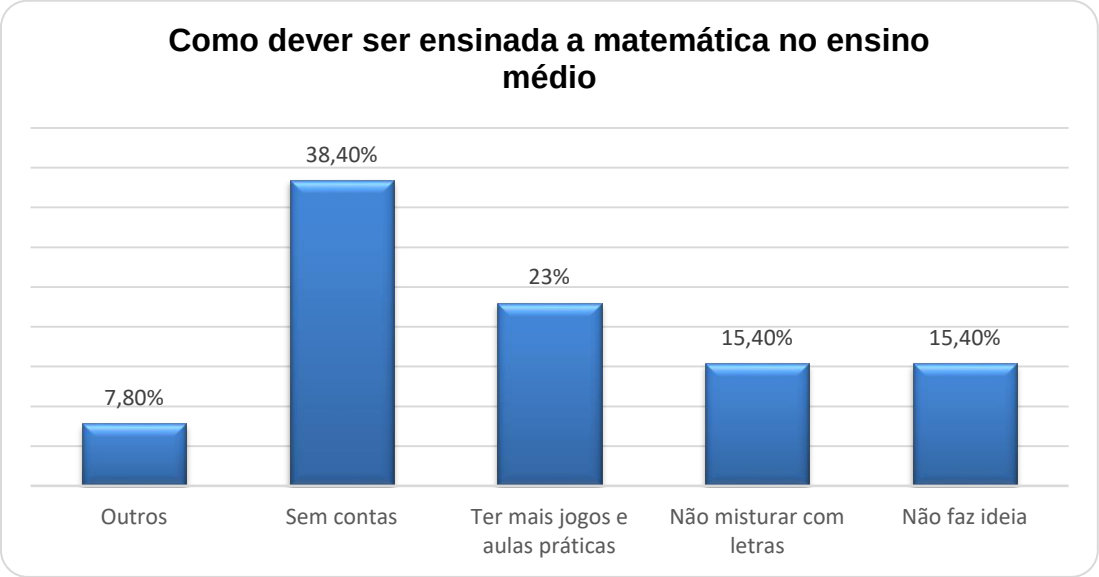
Gráfico 05: Sobre o jogo **RSA-CrypTa**



Fonte: Dados da pesquisa

O Gráfico 06 traz os resultados das opiniões dos alunos de como deveria ser o ensino da matemática no ensino médio. Era esperado que a maioria falasse sobre aulas práticas ou uso de jogos educativos, como o **RSA-CrypTa.**

Gráfico 06: Como a matemática deve ser ensinada no ensino médio



Fonte: Dados da pesquisa

Cerca de 38% afirmaram que o ensino de matemática seria melhor sem a necessidade de fazer contas, 23% que o ensino deveria usar mais jogos e aulas práticas, 5,4% não misturariam letras com números e mais outros 15,4% não fazem ideia de como deveria ser.

Desconsiderando o fato de que 38% não querem que a matemática possua contas, 23% deles afirmaram que seria melhor com o uso de jogos e aulas práticas, justamente o que foi proporcionado a eles com a intervenção do jogo **RSA-CrypTa.**

Os resultados apresentados na seção 5.1 e 5.2 confirmam sua eficácia como intervenção pedagógica. Enquanto os alunos que tiveram acesso ao aplicativo obtiveram um rendimento de 81,3% de desempenho nas *Atividades 01* e *02*, os alunos sem acesso à intervenção registraram rendimento de apenas 53%, mesmo sendo uma turma considerada previamente mais avançada (Tabela 01). Os gráficos também evidenciam a percepção positiva dos alunos em relação ao jogo, com 86,66% deles gostando do aplicativo (Gráfico 03) e 93,33% (Gráfico 04) preferindo aprender matemática de forma prática com jogos ou lúdica.

Destaca-se que 23% dos alunos (Gráfico 07) manifestaram o desejo de que a matemática no ensino médio seja mais voltada para jogos e atividades práticas, revelando uma demanda importante por métodos de ensino mais dinâmicos. No entanto, 38,4% (Gráfico 07) desejaram um ensino sem cálculos e

esse resultado levanta preocupações, uma vez que a ênfase no aprendizado prático não deve excluir o desenvolvimento sólido dos cálculos matemáticos.

A implementação e aplicação do jogo **RSA-CrypTa** obtiveram sucesso, com a participação de 100% dos alunos até o final de todas as fases. Os objetivos propostos, como a manipulação de números inteiros e racionais, o uso de conceitos como *mmc*, *mdc*, *números primos*, *equação do primeiro grau* e o pensamento lógico dedutivo, foram plenamente alcançados, considerando todos os alunos, inclusive os dois estudantes com deficiências que ainda estão em processo de alfabetização.

Por fim, é importante destacar que 73,33% dos alunos gostaram mais da **Fase 03** do jogo (Gráfico 06) relatando, inclusive, ser a fase mais esperada, evidenciando sua curiosidade em decodificar as mensagens trocadas pelos colegas. Esse aspecto demonstra que a motivação e a curiosidade foram impulsionadas pelo jogo ao longo de todo o processo, despertando o interesse dos alunos em aprender.

6 CONCLUSÃO

Um dos grandes desafios encontrados na escola de aplicação do jogo versa sobre o uso indevido do celular em sala de aula. Aliado à dificuldade de aprendizagem matemática apresentada pelos alunos, tornam a vida do professor ainda mais desafiadora.

Diante de tais desafios, a utilização do **RSA-CrypTa** como recurso didático mostrou-se uma promissora solução. Além de combater o problema do uso inadequado dos dispositivos móveis, o jogo demonstrou-se atrativo, motivador e curioso para os alunos, promovendo o aprendizado de conteúdos matemáticos relacionados.

No que tange aos objetivos pretendidos pelo do jogo, todos foram atendidos:

- Teve a sua implementação e execução online bem sucedida com a proposta da exploração da criptografia RSA.
- Os conteúdos matemáticos pretendidos foram abordados e alcançados em níveis distintos de dificuldade.
- Mostrou-se ser uma fonte lúdica de aplicação matemática no mundo moderno, despertando curiosidade e motivação do aluno.
- Possibilitou a criação e aplicação de uma sequência didática em que esteve incluído e usado.

Com base nas observações dos resultados obtidos, a utilização do **RSA-CrypTa** demonstrou-se uma estratégia eficiente e envolvente para lidar com o uso inadequado de celulares em sala de aula, ao mesmo tempo em que promoveu a aprendizagem significativa de conceitos matemáticos e devido ao sucesso dele em sala de aula, será apresentado este ano na Feira de Ciências da escola. Essa abordagem lúdica e prática pode abrir caminho para futuras iniciativas semelhantes, como o melhoramento do jogo, proporcionando uma educação mais engajadora e relevante aos estudantes.

A quem reproduzir a sequência didática apresentada, seria interessante estimular os alunos a conversarem entre si em outros momentos fora da escola, assim a curiosidade de saber o que o colega falou com o outro será mais

contagiante, motivando mais ainda, ao final do processo, o desejo de todos em decodificar as mensagens desejadas. Um aviso: alguns irão ter dificuldade na **Fase 02** e desejarão mudar de diálogo escolhido a fim de encontrarem uma *equação diofantina* mais “fácil”.

O jogo não está perfeito e de forma alguma tem a intenção de exaurir as múltiplas possibilidades de uso. Melhoramentos em sua estrutura e funcionamento ainda são necessárias, como a inserção de uma área para professores com sugestões de uso e modelos de planos de aula acoplados no próprio aplicativo, a sua funcionalidade offline, a escolha do tipo de nível para jogar e um possível compartilhamento de conversas com o Whatssapp, são algumas atualizações que podem ser implementadas e deixariam ainda mais curiosos os estudantes os estimulando a desvendar as fases e aprender mais matemática. A forma como ele contribui para o aprendizado também pode ser estendida com a incorporação de mais assuntos matemáticos para ganho de “vidas” ou privilégios de escapar de fases consideradas mais complexas, como a 02**.** Enfim, há muitas possibilidades de melhoramentos e abrangências que ainda se pode alcançar.

REFERÊNCIAS

ALBUQUERQUE, Rafael Marques; FIALHO, Francisco Antonio Pereira. Concepção de jogos eletrônicos educativos: proposta de processo baseado em dilemas. In: VIII Brazilian Symposium on Games and Digital Entertainment, 2009, Rio de Janeiro. Anais. Rio de Janeiro: Programa de Pós-Graduação em Design e Expressão Gráfica – Brasil, 2009, p. 1-7.

ALMEIDA, M. M. R., INSUCESSO NA MATEMÁTICA: As Percepções dos Alunos e As Percepções dos Professores. Departamento de Ciências da Educação e do Património. Universidade Portucalense. Porto. Março de 2011.

BAHIA. Secretaria da Educação. **Documento Curricular Referencial da Bahia – Etapa do Ensino Médio.** Secretaria da Educação do Estado da Bahia. Salvador, 2020.

BIANCHINI, Edwaldo. Matemática Bianchini 6º ano. 9 ed. São Paulo: Moderna, 2018.

BONJORNO, José Roberto *et al*. Matemática ensino médio – Conjuntos e funções. 1 ed. São Paulo: FTD, 2020.

BOSSELAERS, A., R. Govaerts e J. Vandewalle. 1994. “Comparison of Three Modular Reduction Functions”. Lecture Notes in Computer Science 773:0175–0175.

BRASIL. Ministério da Educação. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. **Relatório Brasil no Pisa 2018.** Versão Preliminar. 2019 Brasília, 2019**.**

BRUXELAS, Ana Catarina. **Aritmética modular e aplicações: criptografia RSA e calendário perpétuo**. 2021. 170 f. Dissertação (Mestrado Profissional em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, Campus São Carlos, São Carlos – SP, 2021.

BURNETT, Steve; PAINE, Stephen. Criptografia e Segurança - O Guia Official RSA. 3 ed. Tradução de Edson Furmankiewicz. Rio de Janeiro: Campus, 2002.

COUTINHO, Severino Collier. Criptografia. 11. ed. Rio de Janeiro: IMPA, 2015

COUTINHO, Severino Collier. Números inteiros e Criptografia RSA. Coleção Matemática e Aplicações. 2. ed. Rio de Janeiro: IMPA, 2014.

DA CUNHA, Jussileno Souza; DA SILVA, José Adgerson Victor. A importância das atividades lúdicas no ensino da matemática. **In: III Escola de Inverno de Educação Matemática – EIEMAT, 2012,** Santa Maria.

DATAREPORTAL. Disponível em: < https://datareportal.com/reports/digital-2022-digital-adoption-doubled-over-the-past-decade?rq=2022>. Acesso em: 21 out.2022.

DIFFIE, Whitfield; HELLMAN, Martin. New Directions in Criptograpy. Ieee Transactions on Information Theory, v. 22, n. 6, p. 644-654, novembro, 1976.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e Matemática.** 2010. 161f. Dissertação (Mestrado em Matemática para Professores) – Universidade de Lisboa, 2010.

HEFEZ, Abramo. Aritmética – Coleção Profmat. 2. Ed. Rio de Janeiro: SBM, 2016.

KNUTH, D. E. 1997. The Art of Computer Programming: Volume 2: Seminumerical Algorithms. 3rd. Addison-Wesley Professional.

KUROSE, James F.; ROSS, Keith W. Redes de computadores e a internet uma abordagem top-down. 6 ed. Tradução de Daniel Vieira. São Paulo: Pearson Education do Brasil, 2013.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de Metodologia Científica. 5. ed. São Paulo: Atlas 2003.

LEAVITT, David. O homem que sabia demais – Alan Turing e a invenção do computador. 2 ed. Tradução de Samuel Dirceu. Ribeirão Preto: Novo Conceito, 2015.

LUZ, Welington Batista. **Introdução à Matemática do Criptossistema RSA**. 2013. 51 f. Dissertação (Mestrado Profissional em Rede Nacional) – Universidade Federal de Sergipe, Campus São Cristóvão, São Cristóvão – SE, 2013.

MADEIRA, Charles et al. Mathmare: Um jogo de plataforma envolvendo desafios matemáticos do ensino médio. In: **Proceedings of the Brazilian Symposium on Computer Games and Digital Entertainment (SBGames 2015). In portuguese**. 2015.

OAK, Ridge National Laboratory. Us department of energy, office of Science, high performance computing facility, operational assessment 2019, oak ridge leadership computing facility. USA, 2020.

OLIVEIRA, Ronielton Rezende. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. Disponível em: <http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf>. Acessado em: 05 jan. 2022.

PASDIORA, Neusa Mara Wanderlinde Leineker. Colégio Estadual São José - Ensino Médio; LAPA–PR, Profissionalizante. Jogos e matemática: uma proposta de trabalho para o Ensino Médio**. Colégio Estadual São José–Ensino Médio e Profissionalizante Lapa–PR, 2008**.

PELLEGRINI, Jerônimo C. Introdução â Criptografia e seus Fundamentos. Notas de aula – Verão: 2019.11.28.20.34. id: e052a0bf8a7589c0c522c6b66cd88eb23. Novembro, 2019.

SCHNEIER, B. 2015. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons.

SELK, Ricardo de Castilho *et al.* **Dimensões - Ciências humanas e sociais aplicadas em diálogo com a matemática.** 1 ed. São Paulo: FTD, 2020.

SILVA, Valéria Batista**. Números primos e criptografia: do conceito ao sistema RSA**. 2019. 88 f. Dissertação (Mestrado Profissional em Rede Nacional) – Universidade Federal de Tocantins, Campus Prof. Dr. Sérgio Jacintho Leonor, Arraias – TO, 2019.

SINGH, Simon Lenha. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. 1 ed. New York: Anchor Books, United States, 1999.

SOUZA, Deivison Porto de; PIRES, Jandersson Dias. Criptoanálise como proposta didática para o ensino de estatística. REnCiMa, v.9, n.2, p.1-11, março, 2018.

SOUZA, Kayodê David de Melo. **Criptografia RSA: Um minicurso para o Ensino Médio.** 2020. 43 f. Dissertação (Mestrado Profissional em Rede Nacional) – Universidade Federal do Espírito Santo, Campus Vitória, Vitória – ES, 2020.

STALLINGS, William. Criptografia e segurança de Redes: princípios e práticas. 6 ed. Tradução de Daniel Vieira. São Paulo: Pearson Education do Brasil, 2014.

VALENTA, Luke et. al. **Factoring as a Service**. University of Pennsylvania, 2015.

ZIMMERMANN, Paul. Fatoração do RSA-250. Cado-nfs-discuss, 2020. Disponível em: < https://sympa.inria.fr/sympa/arc/cado-nfs/2020-02/msg00001.html>. Acesso em 08 mar. 2023.

APÊNDICE A – EXPONENCIAL MODULAR EM C E PYTHON

Algoritmo: **Quadrados Binários** em C

```
int fastExp(int b, int e, int m) {
  int result = 1;

  if (e & 1) {
    result = b;
  }

  while (1) {
    if (!e) {
      break;
    }

    e >>= 1;
    b = (b * b) % m;

    if (e & 1) {
      result = (result * b) % m;
    }
  }

  return result;
}
```

Algoritmo: **Quadrados Binários** em Python

```
def fastExp(b, e, m):
    result = 1

    if e & 1:
        result = b

    while e:
        e >>= 1
        b = (b * b) % m

        if e & 1:
            result = (result * b) % m

    return result
```

APÊNDICE B – SEQUÊNCIA DIDÁTICA

O jogo será online e aplicado a **Turma B** do ensino médio na componente curricular de matemática ou áreas afins[7], em um total de 14 aulas de 50 min cada uma, conforme o Tabela 02. A **Turma A** também teve a mesma sequência de conteúdos, mas sem aplicação ou se quer a menção do jogo.

Tabela 02: Sequência de aulas

Passo	Conteúdo	Recursos Didáticos	Quantidade de aulas
1	Criptografia e o sistema RSA Tabela ASCII	Quadro e pincel Data Show Celular Wifi	02
2	Equação do primeiro grau associado a codificação	Quadro e pincel Data Show	02
3	Números primos e Fatoração	Quadro e pincel Data Show Caderno e caneta	02
4	Raiz quadrada	Quadro e pincel Data Show	01
5	Equação da reta em forma de *equação diofantina*	Quadro e pincel Data Show	04
6	O jogo	Quadro e pincel Data Show Celular ou computador Calculadora Internet Caderno e caneta	03

Fonte: Próprio autor

[7]Referente aos novos componentes curriculares, como Para Além dos Números, inseridas no Novo Ensino Médio por intermédio do Documento Curricular Referencial da Bahia (DCRB).

Criptografia e o Sistema RSA

AULAS 01 e 02

OBJETIVO: Apresentar o que é *criptografia*, seus aspectos históricos, importância atual e sua relação com a matemática e o sistema RSA.

Com o uso do data show, o professor pedirá aos alunos que peguem seus celulares e entrem no site: www.docentes.univasf.edu.br/edson.araujo/rsa, façam o seu registro individual e entrem no jogo. Uma vez dentro do jogo online, o professor deverá pedir ao aluno que converse com alguém logado. Em seguida, pedirá que tentem espionar alguma conversa já iniciada no jogo. Espera-se que eles só vejam números e fiquem curiosos em conhecer o conteúdo das mensagens digitadas.
Uma vez despertada a curiosidades deles, o professor apresentará o que é *criptografia* e alguns de seus principais usos ao longo da história com ênfase à máquina Enigma durante a segunda guerra mundial. Também falar como a *criptografia* é usada atualmente, seu impacto no mundo virtual tendo como exemplo a proteção das transações financeiras via internet e a segurança das conversas em redes sociais, como o Instagram e WhatsApp, e como a maioria dos teclados dos dispositivos eletrônicos ocidentais são orientados segundo a tabela ASCII. Além disso, falar sobre a técnica criptográfica do RSA e como a matemática é usada para ajudar a proteger os dados das pessoas conectadas virtualmente na codificação e decodificação de mensagens. O professor pode sugerir que os alunos assistam ao filme “O Jogo da Imitação”, dirigido por Morten Tyldum com roteito de Graham Moore, onde conta a história de Alan Turing e os desafios com a máquina Enigma e sua criptografia durante a segunda guerra mundial.

RELATO:

Em sala de aula, com o uso da data show, os alunos foram orientados a pegarem seus celulares e entrarem no site: www.docentes.univasf.edu.br/edson.araujo/rsa, para fazerem seu registro individual e entrarem no jogo. Essa tarefa surpreendeu muito a todos, pois o uso indevido do celular nas aulas tem sido uma problemática muito grande na escola, tema inclusive, de exaustivos debates em conselho escolar. Devido a conectividade da internet na

escola, alguns alunos se registraram e entraram rapidamente no jogo e logo estavam conversando entre si através do aplicativo, já outros foram mais lentos e entraram depois. Logo após completarem o registro e conversarem entre si, foram instigados a espionar a conversa dos colegas, o que logo provocou surpresa a curiosidade de todos, pois ninguém conseguia entender o conteúdo das mensagens.

Uma vez despertada a curiosidades deles, foi pedido que clicassem em “Decrypt”, e perceberam que o jogo pedia a resolução de um pequeno problema (Figura 08). A partir daí foi explicado do que se tratava e se deu início a apresentação do que é *criptografia*, alguns de seus principais usos, a tabela ASCII, o sistema RSA e sua relação com o mundo virtual e segurança da internet atrelado às transações comerciais via E-comércio.

Equação do primeiro grau associado a codificação

AULAS 03 e 04

OBJETIVO: Apresentar a pré-codificação e decodificação de um alfabeto comum de **A** a **Z** com letras associadas a números e realizar uma atividade escrita para averiguar o aprendizado.

No quadro, escrever o alfabeto de **A** a **Z** e associar cada letra a algum número de pelo menos dois dígitos. Em seguida, pedir aos alunos que codifiquem no seu caderno a frase, “Todas as cartas de amor são ridículas”, nos números correspondentes a cada letra usada no alfabeto escrito no quadro.

Após a decodificação, fazer o inverso: no quadro, escrever: “Mas mais ridículos são aqueles que nunca escreveram cartas de amor”, codificada nos números do alfabeto escolhido. O aluno não sabe qual é a frase escrita, pois está totalmente em números, ou seja, codificada. Agora ele deve decodificar a frase e torná-la compreensível.

O próximo passo, é mostrar ao aluno que essa forma de abordagem é frágil, pois uma vez sabido o alfabeto principal e sua associação com cada número, qualquer mensagem pode ser compreendida. Nesse sentido, é pedido aos alunos que criem uma equação do primeiro grau onde cada número que correspondem a uma letra do alfabeto esteja colocada no lugar de “x” e, assim, ele encontre seu valor em “y”, ou

seja, “x” será o número a ser codificado e “y” a codificação. Essa estratégia visa não somente mostrar aos alunos que se pode colocar mais coberturas de proteção a uma mensagem, mas como também a dificuldade de algum invasor conhecer a equação de codificação e saber resolvê-la. Em seguida, o aluno revisitará a tabela ASCII e será informado que na próxima aula será revisado conceitos para a assimilação de uma forma muito mais segura de codificar esses números, que é o sistema RSA.

Aproveitando a ideia de usar uma equação do primeiro grau para codificar uma mensagem, o professor aplicará outra atividade (Atividade 01)

RELATO:

Nessas aulas, foi escrito no quadro o alfabeto de **A** a **Z** (Figura 03) onde cada letra foi associada um número de pelo menos dois dígitos e explicado aos alunos como se poderia criar mensagens usando aquele tipo de código. Foi pedido que os alunos codificassem no seu caderno a frase, “Todas as cartas de amor são ridículas”. Em seguida, foi escrito no quadro a frase: “Mas mais ridículos são aqueles que nunca escreveram cartas de amor”, codificada nos números do alfabeto escolhido, e pedido a eles que a decodificassem. Também foi passado uma escrita (Atividade 01) e essa realizada por quase todos, exceto os dois alunos PcDs.

O próximo passo, foi escrever no quadro uma equação de primeiro grau sugerida pelos alunos por instigação do professor, onde nessa equação o “x” representava o número da letra escolhida e o valor de “y”, o número codificado. Assim, a frase “Todas as cartas de amor são ridículas”, foi reescrita na nova forma de codificação e passado para eles uma tarefa para casa e não houve relatos de dificuldade alguma nesse exercício e boa parte deles já estavam operando mentalmente.

Com a aula já findando, revisado, via data show, a tabela ASCII e como ela é aplicada no cotidiano, inclusive pedindo a eles que peguem seus celulares e comparem os caracteres do seu teclado com as da tabela mostrada. Finalmente, foram informados que na próxima aula seria mostrado a eles como uma das formas mais seguras do mundo de se proteger dados funciona, que é a RSA, e que, para isso, se precisaria de alguns conteúdos matemáticos.

Números Primos e Fatoração

AULAS 05 e 06

OBJETIVO: Revisar sobre números primos e compostos e obter uma lista de números primos até 200 ou produzir o *Crivo de Erastóstenes* de 1 a 200 destacando nele os números primos.

Nesta aula, os alunos serão convidados a se juntarem em trio e escreverem no caderno de um deles ou cartolina os números de 1 a 200. Em seguida, riscarão com um “x” todos os múltiplos de 2, depois todos os múltiplos de 3, de 4, de 5 e assim sucessivamente até o 200. Após a tarefa, mostrar a eles que acabaram de recriar o Crivo de Erastóstenes de 1 a 200 e que todos os números não riscados são os números primos e todos os riscados são os números compostos. Se isso não for possível, pode-se mostrar aos alunos uma tabela de primos entre 1 e 200.
Ainda nesta aula, o professor deve pedir aos trios de alunos que escolham dois primos quaisquer da lista e os multiplique entre si, depois peçam a outro trio que tente encontrar quais foram os números usados. Espera-se que os alunos tenham um pouco de dificuldade de fatorar o produto dos dois primos escolhidos e caberá ao professor decidir o uso ou não da calculadora para este fim em específico. Por fim, o professor passará a *Atividade 02* para casa a ser entregue na próxima aula. Essa atividade tem a finalidade de reforçar alguns conceitos matemáticos.

RELATO:

Aqui, os alunos foram divididos em trio para escreverem no caderno os números de 1 a 200. Depois, pausadamente, foi pedido que riscassem com um “x” todos os múltiplos de 2, depois todos os múltiplos de 3, de 4, de 5 e assim sucessivamente até o 200. Em seguida foi perguntado a todos o que seriam os números que não foram riscados e deu-se início a aula sobre números primos e compostos os informando de que tal lista de números se tratava do Crivo de Erastóstenes.

Ainda nesta aula, foi pedido que os trios de alunos que escolhessem dois primos quaisquer da lista que haviam criado e os multiplique entre si. Em seguida,

que pedissem a outro trio que tentasse encontrar quais foram os dois números usados por eles. Essa tarefa demandou tempo, pois muitos não sabiam como fazer, até que uma aluna se destacou e acertou um dos números. Depois disso, ela foi convidada a relatar como os encontrou (foi dividindo o número por outros números aleatórios até que o resultado de um deles fosse inteiro) e, surpreendentemente após a sua fala, todos os demais alunos, com a ajuda de uma calculadora, também encontram os seus números. No fim da aula, foi passado mais um exercício para casa (*Atividade 02*) a ser entregue na próxima aula.

Método da Raíz Quadrada

AULA 07

OBJETIVO: Expor o método da raiz quadrada para encontrar os primos $\boldsymbol{p}$ e $\boldsymbol{q}$ de um número natural $\boldsymbol{n = p \cdot q}$ dado, usando a tabela de primos ou o *Crivo de Erastóstenes* produzido na aula anterior e explorar a **Fase 01** do jogo.

O professor apresentará no quadro o *método da raiz quadrada* para facilitar encontrar os números primos usados em cada trio. Após a apresentação, usar alguns exemplos de produtos de dois primos retirados da **Fase 01** do jogo **RSA-CrypTa** e pedir aos alunos que encontrem a solução usando o método apresentado. Recolher a *Atividade 02* passada na aula passada.

RELATO:

Nesta aula única, foi recolhida a Atividade 02 passada na aula anterior e informado aos alunos de como poderiam encontrar os números primos da aula anterior de forma mais rápida, usando o método da raiz quadrada.

Colocado no quadro diversos produtos entre dois primos quaisquer e pedido a eles que encontrassem esses respectivos números usando o método na raiz quadrada, eles notaram que o universo de números a serem divididos era bem menor do que o que estavam fazendo anteriormente (eles estavam dividindo, por exemplo, 187 por todos os números abaixo de 187). Agora eles estavam dividindo

187 apenas pelos números primos, obtidos no Crivo de Erastóstenes, abaixo ou iguais a 13, que é a aproximação inteira da raiz quadrada de 187. Em seguida, acessaram suas contas no aplicativo e escolheram um diálogo para entrarem da Fase 01 do jogo e passarem dessa etapa usando o *método da raiz* aprendido.

Equação da reta em forma de Equação Diofantina

AULAS 08 a 11

OBJETIVO: Mostrar como resolver uma *equação diofantina* e fazer um paralelo dela com a função afim e a equação da reta.

O professor deverá pedir aos alunos que entrem no jogo e acessem as conversas que estavam na aula anterior e passem para a Fase 02. O objetivo é mostra-los os passos para decodificar em RSA, ou seja, dado uma chave pública $n = p \cdot q$, encontrar os dois primos p e q e resolver a equação diofantina relacionada. Para isso, ele deve revisar sobre mmc e mdc para justificar quando usar a equação diofantina e aproveitar a oportunidade associando essa equação às funções de primeiro grau através da equação da reta.

Primeiramente o professor pedirá aos alunos que encontrem valores inteiros de d e y que satisfaçam a equação:

$$d + y = 100$$

Haverá muitos tipos de respostas para d e y, como 50 e 50, 40 e 60, 30 e 70 e assim por diante.

Em seguida, que resolvam a próxima equação:

$$5d + 300y = 700$$

Novamente, deverão encontrar muitas soluções, como 20 e 2, 100 e 4.

Finalmente, o professor pedirá aos alunos que resolvam a equação

$$2d + 3y = 4$$

Dessa vez, espera-se que os alunos não encontrem valor algum inteiro. O professor deve aproveitar esse exemplo e falar sobre o critério de existência de solução inteira de uma *equação diofantina* linear, isto é, dado $ad + by = c$, para a e b inteiros, se $mdc(a, b) = d$, e d dividir c, então a equação possui soluções inteiras. Do contrário, não existe.

Após essa intermediação, o professor isola y nas duas equações e mostra a relação delas com as funções de primeiro grau e a equação da reta. Em forma de função, é possível encontrar outras tantas soluções esboçando em gráfico, usando a primeira equação dada, $d + y = 100$.

A ideia é mostrar aos alunos que as equações podem possuir uma infinidade de respostas tanto inteiras como até decimais, mas as que procuramos são as soluções inteiras. Ainda nessas equações, o professor apresenta a condição para a solução de uma *equação diofantina*, isto é, valores inteiros. Usando o mdc, ele mostra quando uma *equação diofantina* tem ou não solução e inicia aos alunos como resolver uma equação desse tipo usando exemplos provindos do próprio jogo ao passarem da Fase 01.

RELATO:

Nestas aulas, foi apresentado aos alunos a forma de escrita e existência da equação diofantina e sua relação com a equação da reta e a função de primeiro grau já estudada tanto no nono ano do ensino fundamental II, como no primeiro trimestre da I unidade do 1 ano do ensino médio.

Não houve dificuldade de entendimento da relação entre as duas equações, principalmente na resolução de exemplos simples como $x + y = 100$. No entanto, quando trabalhados coeficientes maiores, como $3x + 9797y = 1$, mais da metade da turma (cerca de 55%) não conseguiu resolver sem ajuda, evidenciando grande dificuldade em sua resolução.

Uma aula foi usada para mostrar a relação da *equação diofantina* com a função e equação de primeiro grau, inclusive usando o Geogebra para mostrar o gráfico dessas funções, e as outras três aulas para a resolução de exemplos diversos. Os exemplos usados foram retirados do ***RSA-Crypta***, Fase 02, já que na

aula anterior eles haviam aprendido e fatorado o número n da Fase 01. Muitos aunos conseguiram avançar nessa etapa, ao passo que outros, não.

O jogo

AULAS 12 a 14

OBJETIVO: Apresentar o jogo e iniciá-lo

Nesta aula, o professor pedirá aos alunos que entrem no jogo online iniciado nas aulas anteriores, entre no diálogo escolhido, espionem e desencriptem a mensagem codificada.

Espera-se que os alunos apliquem o que aprenderam nas aulas anteriores e passem da fase um e dois. Àqueles que não passaram da Fase 02, espera-se que tenham alguma dificuldade nela.

Uma vez passadas dessas duas fases, o aluno se deparará com outro problema: As letras ainda se encontram codificadas. A essa altura, o professor deverá mostrar como encontrar as pistas para desvendar que letras estão associadas a cada número que aparecer na mensagem.

Se o aluno escolher outro diálogo que não vinham trabalhando nas aulas anteriores ou não solucionou ainda a *equação diofantina* da Fase 02 em encontrar o d, o professor deverá ajudá-lo e, se necessário, até calcular junto com ele ou peça que ele se junte a algum colega que já tenha passado dessa fase a fim de que possa compreender como funciona a última parte do jogo. Por fim, após decifrarem o que significa cada número em caractere de um teclado comum de digitação, o sagra-se vencedor do jogo.

RELATO:

Como os alunos já conheciam a interface do jogo, feito o registro, conversado entre si e até tentado desencriptar algumas mensagens codificadas, essas aulas foram para de fato decodificarem.

Após entrarem no jogo pelo celular, como previsto, todos passaram da primeira fase e alguns tiveram grandes dificuldades com a segunda fase. Como nem todos conseguiram encontrar d, que é referente a segunda fase, foi necessário uma

adaptação na forma de aplicação do jogo a fim de que todos pudessem matar a curiosidade de saber como decodifica aquela mensagem que ele esperou tanto para conhecer.

Nesse sentido, a sala foi dividida entre aqueles que conseguiram passar pela segunda fase (12 alunos) e aqueles que não conseguiram (23 alunos)[8]. Os que conseguiram, foram orientados como manusear o leque de letras associadas aos números presentes na conversa escolhida e prosseguiram no jogo. Aos que não conseguiram, foi pedido que todos escolhessem um mesmo diálogo para entrar (Os dois alunos especiais jogaram pelo notebook, ficando apenas na fase 01 e para não ficarem ociosos, foram orientados a entrar em outro diálogo para continuarem a jogar resolvendo a mesma fase e sempre acompanhados pela sua cuidadora). Em seguida, encontraram p e q sem grandes dificuldades e quando chegaram na segunda fase para encontrar d, a *equação diofantina* foi colocada no quadro e resolvida com o professor. Após isso, voltaram às suas conversas anteriormente escolhidas e conseguiram passar da fase 02. Em seguida, foram orientados como manusear o leque de letras associados aos números presentes na conversa. Nesse tempo, os outros alunos já estavam eufóricos com as decifragens das mensagens.

Ao fim da aula, 20 alunos conseguiram resolver dentro do tempo e os 13 restantes resolveram em casa em até 24 horas após a aplicação, enviando as mensagens decodificadas ao professor via internet. Os alunos PcDs concluíram com sucesso a Fase 01 em todos três diálogos diferentes que entraram.

[8] Os dois alunos PcDs não conseguem passar da segunda fase, pois estão no processo de alfabetização.

APÊNDICE C – AVALIAÇÃO DIAGNÓSTICA

OBJETIVO: Avaliar o pré-conhecimento do aluno antes do desenvolvimento das atividades trimestrais.

1. (CEB) Dona Augusta precisava de 850 g de farinha de trigo para fazer um pão e, em casa, só tinha 500 g de farinha de trigo. Teve que comprar um pacote de 1 kg e dele retirar a parte que faltava. Quantos gramas de farinha de trigo sobraram no pacote que Dona Augusta comprou?

a) 250
b) 350
c) 450
d) 650

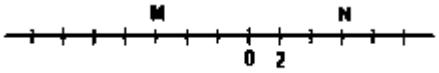
2. Um balde, que pode conter no máximo 2 litros, está com água até a metade de sua capacidade. Sabendo que 1 litro é igual a 1.000 mililitros, quantos mililitros de água há nesse balde?

a) 2000
b) 1000
c) 750
d) 500

3. O conteúdo desta garrafa será distribuído igualmente entre 4 copos com a mesma capacidade. A capacidade máxima de cada copo deverá ser de:

a) 500 mL
b) 450 mL
c) 350 mL
d) 200 Ml

4. (SPAECE). Na reta numérica abaixo, M e N representam números inteiros. Os números correspondentes a M e N, são, respectivamente:

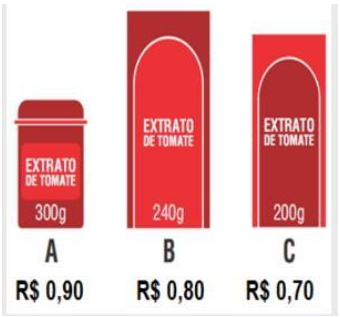


a) -3 e 4
b) -3 e 6
c) -6 e 4
d) -6 e 6

5. (PD-GO) Marcos vai trocar o piso retangular de sua garagem. O pedreiro informou-lhe que cabem 18 peças de cerâmica no comprimento e 15 na largura. Marcos possui 280 dessas peças. Assinale a afirmativa correta de acordo com esta situação:

a) Marcos deverá comprar 10 peças para cobrir todo o piso.
b) Para cobrir o piso, serão necessárias exatamente 280 peças de cerâmica.
c) Após cobrir o piso, ainda sobrarão 10 peças de cerâmica.
d) Marcos deverá comprar 50 peças de cerâmica para cobrir todo o piso.

6. (PD-GO). Vânia precisa de 1.200g de extrato de tomate para fazer um prato especial. Pesquisou o preço de várias marcas, em diversos supermercados, e os produtos mais em conta que encontrou, estão na figura abaixo: Qual dos produtos: A, B ou C ela deve comprar para ter o menor gasto?



a) O mais econômico é o produto A.
b) O mais econômico é o produto B.
c) O mais econômico é o produto C.
d) O gasto é o mesmo na compra de qualquer produto.

7. (PD-GO) A balança abaixo está em equilíbrio, isto é, o peso dos pratos é igual. Considere que cada bolinha pesa 1 quilo e que x representa o peso de cada caixa. Então, a sentença matemática que representa a igualdade dos pesos dos pratos e o valor do peso x de cada caixa são, respectivamente,

a) $7 – x = 4 \rightarrow x = 3$
b) $7 + x = 2 + x \rightarrow x = 9$
c) $7 + x = 2 + 2x \rightarrow x = 9$
d) $7 + x = 2 + 2x \rightarrow x = 5$

8.(SIMAVE). Caio, Ivo e Frederico trabalham como garçons em uma pizzaria. No fim de semana, Caio recebeu R$ 24,50 de gorjeta, Ivo recebeu R$ 28,25 e Frederico recebeu R$ 31,50. Qual foi a quantia total de gorjeta recebida pelos três garçons?

a) R$ 52,75
b) R$ 73,25
c) R$ 74,25
d) R$ 84,25

APÊNDICE D – AVALIAÇÃO COMPARATIVA

ATIVIDADE 01

OBJETIVO: Verificar a aprendizagem sobre mmc, mdc, inclusive a casos contextualizados.

1) Calcule o MMC (mínimo múltiplo comum) dos números abaixo:

a) 12 e 9
b) 21 e 15
c) 12, 15 e 18
d) 15 e 18
e) 36 e 50
f) 15, 20 e 30
g) 50 e 8

2) Rafaela foi ao médico, que receitou dois remédios para ela tomar:

1° remédio: de 6 em 6 horas;
2° remédio: de 8 em 8 horas.

Ela começou a tomar os dois remédios às 08:00 horas da manhã. Qual o próximo horário que ela vai tomar os remédios juntos novamente?

a) 8 h da manhã
b) 12 h da tarde
c) 16 h da tarde
d) 20 h da noite

3) Os planetas Júpiter e Saturno completam uma volta em torno do Sol em aproximadamente 12 e 30 anos respectivamente. Se em certo momento esses planetas se alinham, quantos anos depois eles voltarão a se alinhar novamente?

a) Após 30 anos;
b) Após 42 anos;

c) Após 60 anos;

d) Após 72 anos.

4) Calcule o MDC (máximo divisor comum) dos números abaixo:

a) 40 e 16

b) 120 e 54

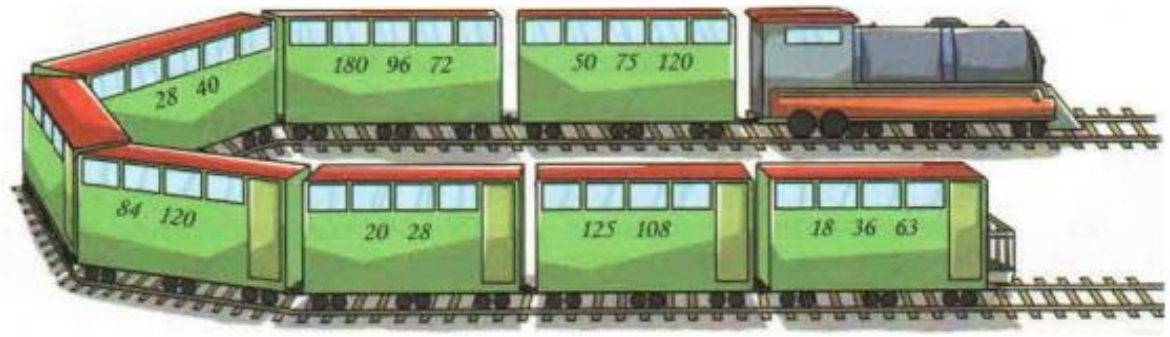
c) 48 e 60

d) 18 e 30

e) 60 e 75

f) 12, 30 e 42

5) Descubra as estações em que o trem vai parar, calculando o MDC dos números pintados em cada vagão. Cada MDC é o número de uma estação em que vai haver parada. Quantas serão as paradas?



ATIVIDADE 02

OBJETIVO: Avaliar a compreensão do aluno acerca de uma contextualização da equação do primeiro grau com criptografia, bem como a fatoração de números inteiros

Questão 01: Usando a equação, $C = 2n + 1$, onde C corresponde ao número codificado e n corresponde ao número associado a letra do alfabeto α, RESPONDA:

Alfabeto α

10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*L*	*M*	*N*

23	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**
O	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*X*	*Z*	*W*	*Y*	*K*

a) Decodifique a seguinte mensagem cifrada:

"5747272155 2155 252153572155 2729 21434753 552147 533727372559412155"

b) Codifique a palavra "**CEMAN**".

Questão 02: Relacione as colunas de cada número à sua fatoração correspondente:

(A) 140 ( ) $3^2.5.11^2$
(B) 500 ( ) $2.5^2.13$
(C) 5445 ( ) $2^2.5.7$
(D) 650 ( ) $2^2.5^3$
(E) 3900 ( ) $2^2.3.5^2.13$

Questão 03: Decomponha em fatores primos os seguintes números:

a) 120
b) 125
c) 143

04: Qual o número cuja fatoração dá:

a) $2.3^2.7^2$?

b) $2^2.3.5^2.7$?

c) $2^2.3.11^2$?

d) $3^2.5.11^2$?

Questão 05: Quando você decompõe 168 em fatores primos, obtém $2^x.3.7$. Qual o valor de x?

Questão 06: Decompondo o número 720 em fatores primos, obtemos $2^4.n.5$. Qual é o fator que você deve colocar no lugar de n para que a forma fatorada represente o número 720?

Questão 07: Qual o m.m.c do número 1**04 e 30**?

Questão 08: Qual é o m.d.c do número 60, 28 e 120**?**

Questão 09: Das sequências abaixo, aquela que **não** contém números primos é:

a) 13, 429, 1029

b)189, 61, 529

c) 2, 111, 169

d) 111, 429, 729

Questão 10: Quais são os números primos entre 50 e 60?

APÊNDICE E – AVALIAÇÃO QUALITATIVA

OBJETIVO: Avaliar o ***RSA-Crypta*** como agente motivador que desperte o interesse e curiosidade do aluno em aprender e aplicar conteúdos matemáticos relacionados ao mundo digital e a matemática aplicada.

1. Você gosta de matemática?

a) SIM
b) NÃO

2. Você já tinha estudado criptografia na escola?

a) Sim
b) Não

3. Você gostou do jogo: ***RSA-Crypta***?

a) SIM
b) Não

4. Que parte do jogo você mais gostou? E a que menos gostou?

_____

_____

5. Qual fase do jogo você considera a mais difícil? Por quê?

FASE 01: Encontrar p e q
FASE 02: Encontrar d
FASE 03: Decifrar os números associados as letras

6. O que você acrescentaria ou tiraria do jogo para o tornar melhor?

_____

_____

07. Como você prefere aprender matemática?

a) Através de jogos
b) Atividades práticas
c) Aulas expositivas com quadro e pincel
d) Outros*

* Se escolheu “outros”, por favor, relate qual seria:

_____
_____

Como acha que deveria ser a matemática no Ensino Médio? Por quê?

_____
_____

Essa questão tem como objetivo entender o nível de motivação dos alunos ao realizarem as atividades propostas, o que impactaria diretamente nos resultados da pesquisa.