Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

RSA-CrypTa: Uma Aplicação da Criptografia no Ensino Médio

Edmarcos M. Jordão[1], Edson L. Araújo[2]
PROFMAT/UNIVASF, Juazeiro, BA

Resumo. O crescimento da internet e da tecnologia aumentou a necessidade de privacidade, levando ao desenvolvimento de métodos de criptografia, como a RSA, baseados em conceitos matemáticos fundamentais. Para ensinar conceitos como *mmc*, *mdc*, números primos e fatoração para alunos do ensino médio, um jogo *online* interativo simulando a interceptação de uma troca de mensagens criptografadas usando RSA foi criado, com sucesso evidenciado pelo rendimento dos alunos e pela percepção positiva do aplicativo, de nome **RSA-CrypTa**.

Palavras-chave. Criptografia, RSA, Jogos *Online*, Ensino, Primos

1 Introdução

Conceitos matemáticos fundamentais, como Mínimo Múltiplo Comum (MMC), Máximo Divisor Comum (MDC) e números primos, são essenciais para a compreensão de uma ampla gama de tópicos em matemática e em outras disciplinas. O MMC, por exemplo, é crucial para a resolução de problemas envolvendo frações e divisão. O MDC, por sua vez, é fundamental para simplificar frações e resolver problemas de divisibilidade. Já os números primos, são a base da teoria dos números, sendo essenciais para a compreensão de conceitos como fatoração e divisibilidade [10].

No entanto, o ensino desses conceitos pode ser desafiador, pois muitos alunos apresentam dificuldade em entender sua aplicação prática e sua relevância para a solução de problemas do cotidiano. Além disso, a complexidade desses conceitos pode dificultar sua compreensão, especialmente em contextos em que são ensinados de forma abstrata e desvinculada de situações reais [1]. De acordo com os dados divulgados pelo Pisa (2019) [5], constatou-se que 68,1% dos estudantes brasileiros em 2018 apresentaram desempenho no Nível 1 ou inferior no que tange às habilidades relativas à matemática.

Assim, estratégias de ensino inovadoras, como o uso de jogos educativos que abordam esses conceitos de forma lúdica e interativa, podem ser uma maneira eficaz de superar essas dificuldades [3, 8, 9]. Esses jogos podem ajudar os alunos a visualizar os conceitos matemáticos em um contexto real, tornando o aprendizado mais significativo e engajador. Por outro lado, a aplicação da criptografia RSA em um jogo pode agregar valor, pois ela encontra-se em uma área de grande interesse e aplicabilidade no mundo real, o que pode aumentar a motivação dos alunos para aprender esses conceitos.

Os objetivos deste trabalho incluem a criação e o teste de um jogo educativo desenvolvido especificamente para o ensino de conceitos matemáticos básicos, MMC, MDC e números primos, utilizando a criptografia RSA como um elemento central. Esta abordagem visa aprimorar a experiência de aprendizado dos alunos, promovendo o engajamento e a compreensão dos conceitos de uma forma lúdica e interativa. Ao integrar a criptografia RSA ao jogo, os alunos são expostos

[1]edmarcosjordao@yahoo.com.br
[2]edson.araujo@univasf.edu.br

aos conceitos matemáticos envolvidos de uma forma acessível e prática. Isso pode aumentar a motivação dos alunos e facilitar a compreensão, bem como promover o desenvolvimento de habilidades cognitivas e analíticas.

2 O Algoritmo RSA

A teoria dos números primos destaca-se como uma das poucas áreas da matemática pura que encontra aplicações práticas no mundo real, especialmente na área da criptografia [11].

Durante os anos 1970, Diffie e Hellman [4] conceberam a ideia de um método matemático simples de utilizar em uma direção, mas extraordinariamente desafiador de aplicar no sentido inverso. Surgia assim, os conceitos de *chave pública* e o método de codificação *assimétrica* [4].

Logo após a introdução do conceito de chave pública por Diffie e Hellman, três jovens matemáticos do Instituto de Tecnologia de Massachusetts (MIT) - Ronald Rivest, Adi Shamir e Leonard Adleman - perceberam que os números primos são a base ideal para a chave perfeita. Esse algoritmo ficou conhecido como **RSA**, derivado das iniciais dos nomes dos seus inventores [2].

2.1 Como funciona o RSA

Sejam p e q dois números primos distintos e um número $m \in \mathbb{N}$, relativamente primo a p e q, simultaneamente, ou seja,

$$\begin{aligned} \text{mdc}(m, p) &= 1 \\ \text{mdc}(m, q) &= 1 \end{aligned}$$

Em tal condição, o **Teorema de Euler-Fermat** [6], garante que

$$m^{(p-1)(q-1)} \equiv 1 \bmod (pq)$$

Deste modo, dados dois números naturais e e d (denominados expoentes de encriptação e desencriptação, respectivamente), tais que

$$ed \equiv 1 \bmod \Big((p-1)(q-1) \Big) \tag{1}$$

tem-se que

$$\begin{aligned} \left(m^e\right)^d \bmod (pq) &= \left(m^{ed}\right) \bmod (pq) \\ &= m \bmod (pq) \end{aligned}$$

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

$$m \equiv \left(m^e\right)^d \bmod (pq)$$

Em outras palavras, entendendo-se m como uma mensagem que deseja-se proteger, de posse do par de números (e, n) (*chave pública*), sendo $n = pq$, tem-se a *mensagem criptografada* dada por

$$m^e \bmod (n)$$

e através do par (d, n) (*chave privada*), é possível *descriptografar* tal mensagem, tendo em vista que

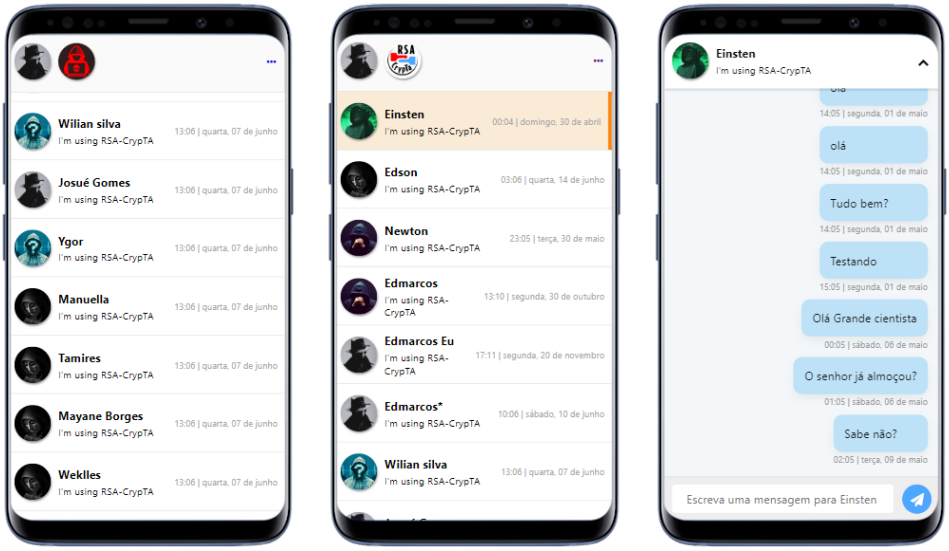
$$m \equiv \left(m^e\right)^d \bmod (n)$$

DOI: 10.5540/03.2025.011.01.0473

3 Aplicativo

No avançado mundo tecnológico atual, a educação está constantemente se reinventando para se adaptar às necessidades e preferências dos alunos. Neste contexto, foi desenvolvido, como parte deste trabalho um jogo *online*[3] inovador, nomeado **RSA-CrypTa**, projetado para ensinar conceitos matemáticos essenciais de forma envolvente e interativa. Este jogo, disponível gratuitamente mediante cadastro, é acessível em uma variedade de dispositivos, desde celulares até computadores pessoais que disponham de um navegador, oferecendo flexibilidade e conveniência aos usuários. Seu objetivo principal é transformar a aprendizagem de tópicos como MMC, MDC e números primos em uma experiência atraente, simulando a interceptação de uma conversa criptografada utilizando o algoritmo RSA. Esta abordagem pretende inovar a forma como os estudantes abordam e compreendem a matemática, ao mesmo tempo em que oferece uma nova dimensão de ensino.

O **RSA-CrypTa** possui duas interfaces: o modo *bate-papo* (Fig. 1a) e *modo hacker* (Fig 1b). No modo *bate-papo* os usuários podem trocar mensagens entre si, simulando um aplicativo de mensagens semelhante ao *Whatsapp* ou *Telegram* (Fig. 1c). As mensagens trocadas nesta área serão o alvo da interceptação, objetivo principal do jogo.



(a) *Modo Bate-papo* (b) *Modo Hacker* (c) *Uma conversa*

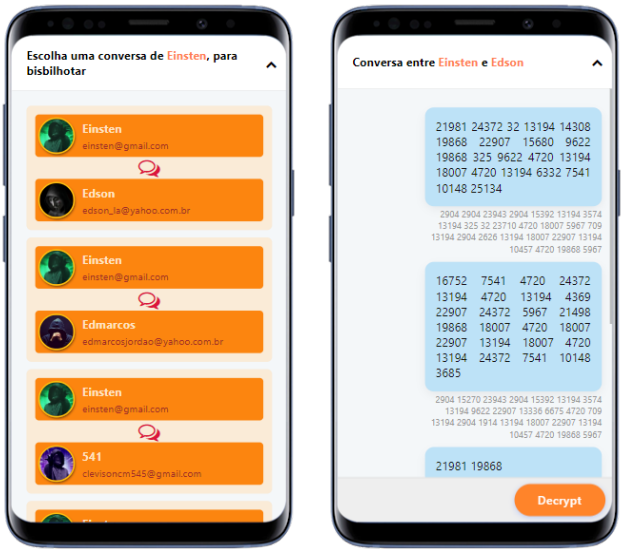
Figura 1: Os dois modos de uso do **RSA-CrypTa**. Fonte: Autores.

No *modo hacker*, que consiste no jogo em si, o usuário será desafiado em três etapas, que seriam as fases do jogo.

Inicialmente o usuário deve escolher outro usuário que será alvo de sua interceptação (nesta escolha, entendemos que não faz sentido interceptar mensagens nas quais o próprio usuário faz parte da conversa, e deste modo, somente mensagens entre os outros usuários aparecem como opções de escolha) (Fig. 2a).

[3]Disponível em http://www.docentes.univasf.edu.br/edson.araujo/rsa

DOI: 10.5540/03.2025.011.01.0473



(a) (b)

Figura 2: Selecionando uma conversa para interceptar. (a) Conversas disponíveis. (b) Conversa escolhida em sua versão criptografada. Fonte: Autores.

Ao escolher uma conversa, o aplicativo exibirá ao interceptador a versão criptografada da mesma e um botão que permite seguir para a primeira etapa do jogo: descobrir os primos p e q (Fig 2b).

1^a Fase

Nesta etapa, o interceptador é informado da *chave pública* (e, n) e é desafiado a descobrir os valores de p e q tais que $p\,q = n$ (Fig. 3a). Para que esta tarefa seja possível para estudantes do ensino médio, o aplicativo usou uma criptografia de 16 bits apenas, permitindo o uso de números primos relativamente pequenos. A ideia é que para descobrir p e q, o aluno faça uso dos *critérios de divisibilidade* ou do *Crivo de Erastótenes*, por exemplo.

Ao descobrir os valores de p e q, o botão de envio (Fig. 3a) tornar-se verde indicando que a resposta está correta e permite ao usuário seguir para a fase seguinte.

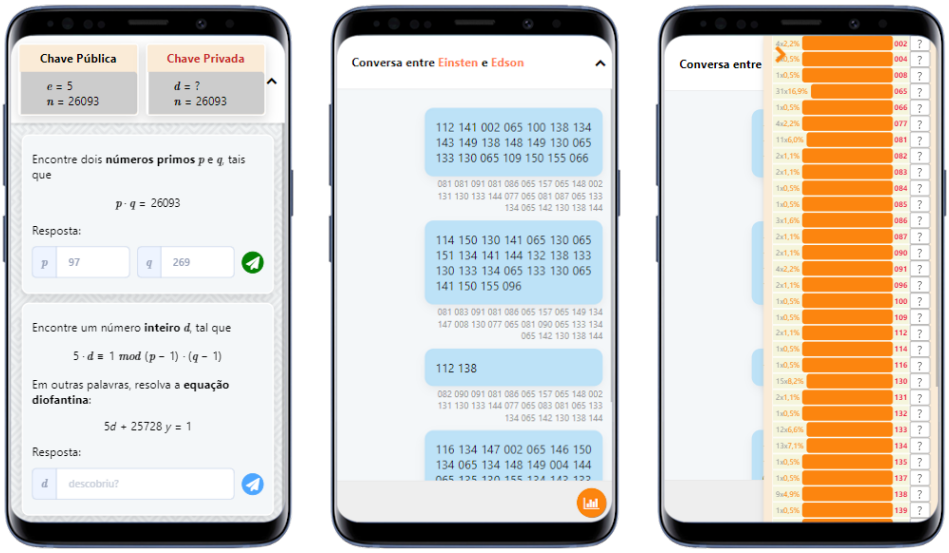
2^a Fase

Neste momento, o usuário será apresentado à *equação diofantina* construída a partir de p e q encontrados na fase anterior e equivalente à equação (1) (Fig. 3a), cuja solução permite encontrar o *expoente de desencriptação* d. Esta equação admite infinitas respostas e qualquer uma delas é aceita pelo **RSA-CrypTa**. Embora equações diofantinas não façam parte do currículo escolar, sua semelhança com a equação da reta e uma breve introdução ao processo de resolução conduzem o aluno a aplicação de conceitos como MMC, MDC, divisibilidade e aritmética básica.

3^a Fase

Na terceira e última fase, posta no jogo apenas para torná-lo mais atrativo e também permitindo aos estudantes um primeiro contato com a estatística, a mensagem será apresentada desencriptada mas, ainda no formato numérico (Fig. 3b) porém, tendo cada caractere deslocado de acordo com a *Cifra de César*. O estudante poderá realizar inferências com base nos percentuais de frequência de cada um dos caracteres (Fig. 3c), ou mesmo se utilizar de padrões reconhecíveis nas mensagens trocadas em outro momento na área de bate-papo.

DOI: 10.5540/03.2025.011.01.0473



(a) (b) (c)

Figura 3: (a) Fases 1 e 2. (b) Conversa descriptografada, versão numérica. (c) Frequências. Fonte: Autores.

4 Metodologia

Para avaliar a eficácia do jogo educativo **RSA-CrypTa**, foram selecionadas duas turmas do primeiro ano do ensino médio na *Escola Estadual de Tempo Integral Manoel Novaes*, situada em Curaçá, Bahia. A **Turma A**, composta por 31 alunos, e a **Turma B**, composta por 35 alunos, foram submetidas a uma avaliação inicial para diagnóstico (Apêndice C, [7]). A **Turma B**, identificada em um estágio de desempenho inferior, foi escolhida para participar da intervenção com o **RSA-CrypTa**, enquanto a **Turma A** seguiu o método tradicional de ensino. Uma sequência didática foi elaborada (Apêndice B, [7]) para abordar o conteúdo relacionado ao **RSA-CrypTa** na **Turma B**, enquanto o mesmo conteúdo foi ensinado de forma convencional na **Turma A**. Para avaliar a eficácia comparativa, ambos os grupos foram submetidos a dois questionários (Apêndice D, [7]). Além disso, um questionário qualitativo (Apêndice E, [7]) foi aplicado exclusivamente à **Turma B** para explorar as percepções dos alunos em relação ao jogo educativo. Essa abordagem metodológica permite uma análise abrangente e comparativa dos resultados obtidos com o uso do **RSA-CrypTa** em relação ao ensino tradicional, além de fornecer *insights* valiosos sobre a experiência dos alunos com a ferramenta educacional.

5 Resultados

Os resultados deste estudo revelam diferenças marcantes entre as turmas A e B, evidenciando o impacto positivo do jogo **RSA-CrypTa** no processo de aprendizagem dos alunos. A avaliação diagnóstica inicial demonstrou que a **Turma A** apresentava um desempenho superior, com um percentual de acertos de 76%, enquanto a **Turma B** registrou apenas 48% de acertos na atividade de sondagem aplicada. Após a implementação da sequência didática, a avaliação comparativa revelou uma melhoria significativa no desempenho da **Turma B** em relação à **Turma A**. Em duas atividades avaliativas, com 5 e 10 questões, respectivamente, a **Turma B** obteve um percentual

de acertos superior em 12 das questões(Fig. 4), demonstrando assim a eficácia do **RSA-CrypTa** como ferramenta de ensino.

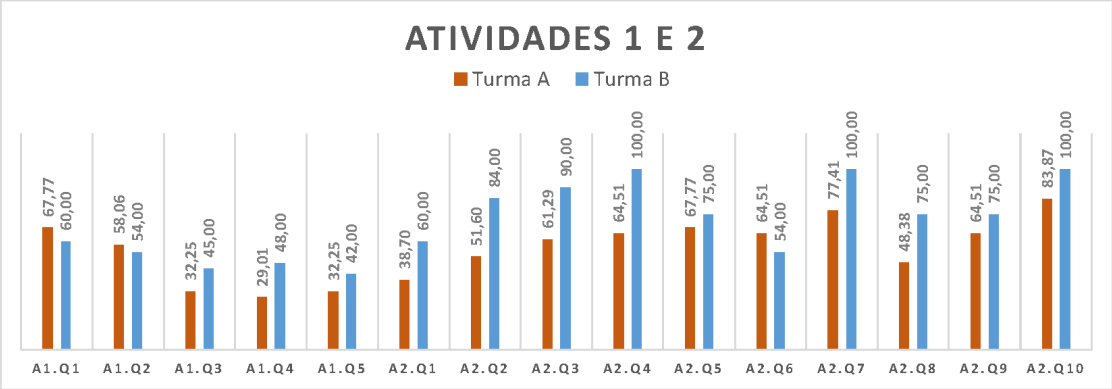


Figura 4: Atividade 01 (A1.Q1 a A1.Q5) e Atividade 02 (A2.Q1 a A2.Q10). Fonte: Autores.

Além dos resultados quantitativos, a percepção dos alunos sobre o jogo também foi investigada. Os dados revelaram que o **RSA-CrypTa** foi bem recebido pelos alunos, com uma alta taxa de participação e engajamento nas diferentes fases do jogo. Na primeira fase, todos os 35 alunos completaram a tarefa, sendo que a maioria deles conseguiu finalizá-la em até 5 minutos. Nas fases subsequentes, observou-se uma redução no número de participantes, mas ainda assim uma parcela significativa dos alunos conseguiu completar as tarefas dentro do tempo previsto. É importante ressaltar que a maioria dos alunos não tinha experiência prévia em criptografia, o que ressalta a capacidade do **RSA-CrypTa** de despertar interesse e curiosidade mesmo em temas não familiares.

A análise das respostas dos alunos também revelou *insights* interessantes. A fase 2 foi considerada a mais desafiadora, principalmente devido à quantidade de cálculos envolvidos, enquanto a fase 3 despertou grande expectativa entre os alunos, que estavam ansiosos para descobrir o conteúdo das mensagens encriptadas. Além disso, mais de 93% dos alunos expressaram preferência por aulas práticas ou com jogos para o ensino de matemática, destacando a importância de abordagens educativas inovadoras e envolventes.

Esses resultados apontam para o potencial do **RSA-CrypTa** como uma ferramenta eficaz para o ensino de matemática, proporcionando não apenas uma melhoria no desempenho acadêmico dos alunos, mas também estimulando o interesse e a motivação pelo aprendizado.

6 Conclusões

Com base nos resultados obtidos neste estudo, é possível afirmar que **RSA-CrypTa** apresenta um impacto positivo e significativo no ambiente escolar. Em primeiro lugar, verificou-se que o jogo foi eficaz na redução do uso indevido de celulares em sala de aula, além de combater a desmotivação em relação à matemática. Sua abordagem atrativa, motivadora e curiosa estimulou o interesse, resultando em uma maior participação e engajamento durante as atividades relacionadas. A integração do **RSA-CrypTa** na sequência didática proporcionou uma nova e eficaz abordagem no ensino, promovendo uma aprendizagem significativa e duradoura. Além disso, o jogo serve como um modelo para iniciativas futuras, abrindo caminhos para o desenvolvimento de recursos educacionais semelhantes. É importante ressaltar que o **RSA-CrypTa** ainda permite melhorias, como a inclusão de uma área para sugestões de professores e a implementação de diferentes níveis de dificuldade, visando aprimorar ainda mais sua utilidade e eficácia no contexto educacional.

DOI: 10.5540/03.2025.011.01.0473

Agradecimentos

Gostaria de expressar minha profunda gratidão ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) pelo apoio e oportunidade concedidos durante o desenvolvimento deste trabalho. Agradeço à Universidade Federal do Vale do São Francisco (UNIVASF) por sediar e proporcionar os recursos necessários para a realização deste projeto. Ao meu orientador, o prof. Edson L. Araújo, pelo seu empenho, paciência e orientação constante, que foram fundamentais para o sucesso deste estudo. Aos meus colegas do PROFMAT, pelo compartilhamento de ideias, troca de experiências e pelo suporte mútuo ao longo deste período. Por fim, agradeço a Deus, que me concedeu força e sabedoria para superar os desafios e me conduziu até aqui. Sem o apoio e a colaboração de todos esses agentes, este trabalho não teria sido possível.

Referências

[1] M. M. R. Almeida. "Insucesso na matemática: as percepções dos alunos e as percepções dos professores". Dissertação de mestrado. Porto: Universidade Portucalense, 2011.

[2] S. C. Coutinho. **Números inteiros e criptografia RSA**. 2a. ed. Coleção Matemática e Aplicações. Rio de Janeiro: IMPA, 2014.

[3] J. S. da Cunha, D. Silva e J. A. Victor. **A importância das atividades lúdicas no ensino da Matemática**. Apresentado na III Escola de Inverno de Educação Matemática – EIEMAT, Santa Maria. 2012.

[4] W. Diffie e M. Hellman. "New directions in cryptography". Em: **IEEE Transactions on Information Theory** 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[5] BRASIL. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira. **Relatório Brasil no PISA 2018**. Rel. técn. Paris: OCDE Publishing, 2019. URL: http://portal.inep.gov.br/pisa-no-brasil.

[6] A. Hefez. **Aritmética, Coleção PROFMAT**. 2nd. Rio de Janeiro, RJ: Sociedade Brasileira de Matemática, 2016. ISBN: 978-85-8337-181-6.

[7] E. M. Jordão e E. L. Araújo. "RSA-CrypTa: Uma Aplicação da Criptografia no Ensino Médio". Dissertação de mestrado. PROFMAT, Juazeiro, BA: Universidade Federal do Vale do São Francisco, Agosto de 2023.

[8] C. Madeira, L. Câmara, I. Beserra e R. Tavares. "Mathmare: um jogo de plataforma envolvendo desafios matemáticos do ensino médio". Em: **Proceedings of the Brazilian Symposium on Computer Games and Digital Entertainment (SBGames 2015). In portuguese**. 2015.

[9] N. M. W. L. Pasdiora. "Jogos e matemática: uma proposta de trabalho para o Ensino Médio". Em: **Colégio Estadual São José–Ensino Médio e Profissionalizante Lapa–PR** (2008).

[10] K. H. Rosen. **Elementary number theory and its applications**. 6a. ed. Pearson, 2010. ISBN: 978-0-321-50031-1.

[11] S. Singh. **The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography**. 1a. ed. New York: Anchor Books, 1999.

