CRIANDO CÓDIGOS CRIPTOGRÁFICOS: UMA PROPOSTA PARA O USO DA CRIPTOGRAFIA RSA *(RIVEST-SHAMIR-ADLEMAN)* PARA O ESTUDO DE NÚMEROS PRIMOS E ARITMÉTICA MODULAR

Anderson de Araújo BARROS[1]
Jeane Gardênia Costa do NASCIMENTO[2]

RESUMO

O presente trabalho propõe a abordagem da criptografia RSA (*Rivest-Shamir-Adleman*), criptografia esta que por sua vez que está relacionada a uma grande variedade de transações eletrônicas que envolvem transferências financeiras e mensagens sigilosas onde a matemática é a principal ferramenta para esse fim. Para dar corpo a pesquisa buscou-se junto à literatura pertinente entender como processos criptográficos ocorreram ao longo da história e verificar a possibilidade de utilização da criptografia RSA como elemento motivador ao estudo de números inteiros, em especial números primos, decomposição de números compostos, divisão de números inteiros e aritmética modular, sendo a última apresentada de forma intuitiva, fato que harmonizou o estudo aqui apresentado como pesquisa bibliográfica. Resultados apontaram que é possível trabalhar o tema desde que este seja bem conduzido pelo professor sendo a mesma figura central para a apresentação de maneira leve e didática da proposta.

Palavras-chave: Criptografia. Matemática. Criptografia RSA. Teoria dos números.

ABSTRACT

The current study frame approach sugest in the encryption RSA (Rivest-Shamir-Adleman) encryption approach, which in turn is kindred to a wide range of electronic transactions involving financial transfers and sensitive messages where mathematics is the main tool for this purpose. To give substance to the research, we sought to understand how cryptographic processes occurred throughout history and to verify the possibility of by employing RSA cryptography as a motivating element for the study of whole numbers, presentarly prime numbers, decomposition of compound numbers, division. Integers and modular arithmetic, the latter being presented in an intuitive way, a fact that harmonized the study by employing here as bibliographical research. Results showed that it on the possibility to works on the theme as long as it is well conducted by the teacher, being the any head represented for by employing of the proposal in a light and didactic proposed.

Keywords: Encryption. Math. RSA Encryption. Number theory.

[1]Licenciando do curso de Licenciatura em Matemática, Instituto Federal Piauí (IFPI), campus Teresina Central. Teresina, Piauí, Brasil. E-mail: barrosanderson1920@gmail.com
[2]Mestre em Ensino de Ciências e Matemática, Professora do Instituto Federal do Piauí (IFPI), campus Teresina Central. Teresina, Piauí, Brasil. E-mail: jeane.gardenia@ifpi.edu.br.

Keywords: Cryptography. Mathematics. RSA encryption. Number theory

1 INTRODUÇÃO

Apesar dos avanços pedagógicos nas últimas décadas, ainda é possível identificar as dificuldades enfrentadas tanto por professores, para ensinar, quanto para os estudantes em aprender a matemática, fato que possivelmente tem origem na falta de clareza em relação a aplicação da matemática na realidade. Na aritmética, por exemplo, podemos destacar a não aplicação na realidade da decomposição de um número composto em fatores primos bem como do resto da divisão entre dois números.

Sobre essa problemática, Haidt (1999, p. 75) reforça que “para que haja uma aprendizagem efetiva e duradoura é preciso que existam propósitos definidos e auto atividade reflexiva dos alunos”. O estudo dos números, as relações entre os mesmos e suas propriedades são imprescindíveis para o aprendizado efetivo dos conteúdos matemáticos propostos visto que estes estão diretamente relacionados ao desenvolvimento tecnológico.

O avanço tecnológico ao qual estamos vivenciando diariamente exige constantemente a rápida e segura troca de informações entre os usuários, como é o caso da internet, e a segurança dessas informações exige métodos de proteção contra a apropriação indevida de informações. A criptografia RSA é um desses métodos de proteção e está relacionado diretamente com aritmética dos restos e ao processo de fatoração de números compostos.

D’Ambrósio (1991) afirma que “(...) há algo de errado com a matemática que estamos ensinando. O conteúdo que tentamos passar adiante através dos sistemas escolares é obsoleto, desinteressante e inútil”. Ou seja, sem qualquer contextualização ou articulação mais profunda com o cotidiano dos estudantes, o que propicia a inexistência efetiva de um bom aprendizado.

> Se a matemática é uma disciplina base de todas as ciências e todas as artes; se o domínio dos números e das operações é decisivo para o sucesso numa sociedade competitiva; se o desenvolvimento tecnológico está fundamentado em cálculos e logaritmos; se o Brasil é a terra de Malba Tahan… por que 89% dos estudantes chegam ao final do Ensino Médio sem aprender matemática? (LORENZI, 2008)

Faz-se necessária uma profunda discussão e principalmente a busca por respostas sobre os reais motivos de a matemática apresentar tantas rupturas, contudo alguns desses motivos podem estar relacionados à insuficiente fundamentação aritmética tão notória entre a classe estudantil.

A aritmética, assim como a matemática como um todo, necessita de recursos de ensino mais voltados e interligados ao mundo tecnológico permitindo uma real integração da escola ao cotidiano favorecendo assim a real aprendizagem. A Base Nacional Comum Curricular (BNCC) defende que:

> Os estudantes utilizam tecnologias, como calculadoras e planilhas eletrônicas, desde os anos iniciais do Ensino Fundamental. Tal valorização possibilita que, ao chegarem aos anos finais, eles possam ser estimulados a desenvolver o pensamento computacional, por meio da interpretação e da elaboração de fluxogramas e algoritmos.
> — Em continuidade a essas aprendizagens, no Ensino Médio o foco é a construção de uma visão integrada da Matemática, aplicada à realidade, conforme anteriormente anunciado. Nesse contexto, quando a realidade é a referência, é preciso levar em conta as vivências cotidianas dos estudantes do Ensino Médio, envolvidos, em diferentes graus dados por suas condições socioeconômicas, pelos avanços tecnológicos, pelas exigências do mercado de trabalho, pela potencialidade das mídias sociais, entre outros.

Norteados por essa discussão entende-se que o professor ao proporcionar aos estudantes, quando possível, sua inserção no mundo das técnicas para criptografia de mensagens, mesmo simplificadas, estará integrando de forma efetiva a matemática ao cotidiano, permitindo ao estudante entender processos realizados por computadores e até mesmo pelo seu aparelho celular estimulando a pesquisa e o gosto pela matemática.

2 CRIPTOGRAFIA E A HUMANIDADE

Por muitos séculos a comunicação escrita tem sido a forma de mostrar no presente todo um passado, por mais distante que esse seja. A escrita foi uma das maiores, se não a maior, invenção do homem. A linguagem também é uma maneira de comunicação, porém considerada instável, em sua transmissão ocorre o risco de se modificar, já a escrita permanece imutável. Em dado momento surgiu à

necessidade de uma transmissão segura de mensagens, onde apenas o emissor e o receptor poderiam ter acesso ao conteúdo, temos então os primeiros passos da criptografia, sendo esta a área do conhecimento que produz técnicas que permitem a transmissão segura de mensagens.

Motivos não faltaram para o ser humano necessitar codificar e decodificar mensagens; segredos militares, políticos, religiosos entre outros. Simon Singh em O Livro dos códigos descreve que: “Durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos”. (1999, p.1)

Durante a segunda guerra mundial foram desenvolvidas muitas tecnologias com objetivos militares, desde armas modificadas até máquinas para codificação de mensagens. A máquina Enigma é um exemplo mais significativo desse tipo de tecnologia e evidenciou ainda mais a importância da criptografia para a dinâmica da guerra.

Por volta de 2000 a.C, Egito e Mesopotâmia foram o palco para as primeiras aparições da criptografia. Os sacerdotes egípcios utilizaram a escrita hierática, não compreendida pela população que fazia o uso de uma linguagem mais simples. Os sumérios, na Babilônia, faziam o uso da escrita cuneiforme que era ideográfica e fonética.

Alecrim (2005, p.1) explica que o surgimento da palavra Criptografia ocorreu com a união de palavras, em grego, “Kryptós” e “gráphein”, que significam “ocultos” e “escrever”, respectivamente.

Na atualidade, ao fazermos uma transação bancária ou mesmo uma compra um bem via internet, os dados utilizados devem ser protegidos de possíveis fraudes e nesse processo sigiloso a criptografia tem papel primordial. Códigos baseados em números primos são empregados na segurança que se baseia na dificuldade de encontrar os fatores primos de um dado número que é um processo bastante complicado, Eves (2005, p.662), por exemplo, pontua que “Os números primos ostentam uma longa história desde os gregos antigos até o presente […]”.

O teorema fundamental da aritmética diz que os números primos são tijolos de construção a partir dos quais os outros inteiros são formados multiplicativamente.

Esses números foram muito estudados em um grande esforço para determinar a natureza de sua distribuição nas sequências dos inteiros positivos,

sendo muito úteis na criptografia para criação de senhas (chaves) e assim proteger dados confidenciais.

Segundo Coutinho: “A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos “códigos secretos”. (2008, p.1). Existe um sistema de números em que os gregos antigos denominavam como um sistema cifrado, chamado sistema de numeração Jônico ou alfabético. Sobre este sistema, Eves comenta que: “[...] é um exemplo de sistema cifrado”. Ele é decimal e emprega 27 caracteres – as 24 letras do alfabeto grego mais três outras obsoletas: *digamma, koppa e sampi*.” (2004, p.35).

A criptografia trata-se, portanto, de um conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consigam decifrá-la e para isso, várias técnicas são usadas e com o passar do tempo modificado, aperfeiçoado de maneira que se tornem cada vez mais seguras.

Para um sistema criptográfico funcionar adequadamente deve cumprir com duas exigências:

- *Reversibilidade*, ou seja, se alguma informação for codificada, tem que ser possível desfazer esta codificação, caso contrário à informação é transformado e ninguém conseguirá voltar à informação original, por isto é necessário que este sistema permita desfazer àquilo que foi feito.
- *Chave*, que será usada para decodificar aquilo que foi codificado, se o receptor ele não possuir esta chave, não conseguirá entender o que foi dito.

Um bom exemplo disso está em um método bastante simples bem difundido principalmente entre crianças e adolescentes de associar a cada letra do alfabeto um número e enviando mensagens numéricas baseadas nesse código, tanto quem envia quanto quem recebe devem conhecer o “segredo” codificando e decodificando a mensagem de maneira a evitar ambiguidades.

2.1 A Criptografia RSA

O método de criptografia RSA, foco dessa pesquisa, parte de um princípio aparentemente simples, mas que exige ferramentas bem mais sofisticadas de decodificação visto que exige um trabalho com números primos e através do produto

desses números a criação de uma chave de codificação da mensagem, chamada chave pública. Esse procedimento é realizado com números primos muito grande de modo que quem conhece a chave pública dificilmente conseguirá identificar os números primos utilizados e decodificar a mensagem.

A criptografia RSA foi desenvolvida em 1977 por L. Rivest, A. Shamir e L. Adleman, todos os funcionários da *Massachussets Institute of Technology* (M.I.T.) que é uma das mais importantes universidades americanas. O nome do método representa as letras iniciais dos nomes dos criadores. O matemático Leonard Adleman validava as ideias dos desenvolvedores pelo ponto de vista matemático e em 1977 os três registraram a patente do método RSA.

O método RSA foi desenvolvido baseado em uma das áreas mais elementares da matemática, a teoria dos números. A dificuldade em decompor um número em seus fatores primos é fator determinante para a segurança do método. Uma chave segura em RSA é gerada a partir da multiplicação de números primos de cerca de 200 algarismos cada e assim a fatoração desse número se torna algo que levaria bastante tempo, mesmo que essa fatoração seja feita por potentes computadores.

2.2 O algoritmo de Euclides

O Algoritmo de Euclides é um dos algoritmos mais antigos que se tem conhecimento (data de cerca de 300 a.C) e pode ser encontrado no Livro VII da obra *Os Elementos* de Euclides. Ainda nos dias de hoje, o Algoritmo de Euclides é uma das maneiras mais simples e eficientes de se calcular o MDC. O procedimento é também conhecido como processo das divisões sucessivas, pois é a partir de sucessivas divisões que ele é executado, e baseia-se no seguinte resultado:

Sejam a e b números naturais, com $a > b > 0$. Se q e r são, respectivamente, o quociente e resto da divisão de a por b, então $mdc(a, b) = mdc(b, r)$.

2.3 Aritmética modular

A teoria dos números abrange vários conteúdos elementares da matemática, a aritmética modular é um deles e contempla muitos conceitos importantes. Os

teoremas e propriedades envolvidos no seu estudo vão desde assuntos da educação básica a assuntos mais complexos. Como o trabalho em questão acrescenta técnicas e metodologias a serem aplicadas em sala de aula pelo professor, serão abordados apenas conteúdos essenciais para esse objetivo. A aritmética modular estar fundamentada na seguinte definição:

Sejam dois números naturais *a* e *b* que, depois de efetuadas as divisões por um número natural *m*, não nulo, por meio do algoritmo de Euclides, produzem o mesmo resto. É dito então que "*a* é congruente a *b* módulo *m*". Ou:

$$a \equiv b(mod m)$$

3 METODOLOGIA

Objetivando propor a utilização da criptografia RSA em uma abordagem para a utilização de primos e decomposição de números compostos, o presente trabalho referenciou-se em pesquisas na literatura disponível acerca do tema. Tal abordagem permitiu a classificação do presente estudo como uma pesquisa bibliográfica.

A pesquisa bibliográfica segundo afirma Severino (2007, p.122) "é aquela que se realizam a partir do registro disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, artigos, teses, etc.".

O que se enquadra perfeitamente ao estudo aqui apresentado, pois todos os dados presentes são oriundos de livros, teses, dissertações e monografias de graduação. Sendo obrigatória nos trabalhos científicos, a pesquisa bibliográfica é o meio que torna conhecida a produção científica existente.

Beuren e Raupp (2004, p.87) ainda esclarecem que:

> O estudante, na elaboração do trabalho monográfico, sempre se valerá desse tipo de pesquisa, notadamente por ter que reservar um capítulo do trabalho para reunir a teoria condizente com seu estudo, normalmente chamado de revisão de literatura ou fundamentação teórica.

Passe agora à descrição de uma proposta de atividade que tem como base os pressupostos da criptografia RSA.

Primeiramente, percebeu-se a necessidade de oferecer ao professor uma espécie de roteiro para a aplicação da atividade em sala de aula haja vista a mesma não se enquadra em uma atividade usualmente trabalhada, de modo que propomos que ao início da aula seja feita uma explanação sobre a criptografia, apresentando seu contexto histórico e importância no decorrer da evolução tecnológica, os tipos de criptografias existentes, dando ênfase à criptografia RSA e seu uso atual na sociedade, tais informações serão o fator motivador para a próxima etapa.

Após o momento de contextualização histórica faz-se oportuna à revisão e/ou apresentação dos conteúdos matemáticos necessários para a execução da atividade sendo estes: decomposição de números inteiros em fatores primos e estudo dos restos ou aritmética modular, este último tópico deverá ter uma abordagem intuitiva, com exposição da definição e alguma das propriedades da aritmética modular, exemplos de aplicações dessas propriedades e exercícios para fixação do conteúdo ministrado.

A etapa seguinte é a de aplicação prática dos conteúdos estudados para a codificação e decodificação de mensagens utilizando o mecanismo de criptografia RSA. Esse mecanismo será dividido em duas partes, a primeira, que compreende a pré-codificação e codificação da mensagem, a segunda, compreende a decodificação da mesma mensagem codificada na etapa anterior.

Para exemplificar o processo de codificação e decodificação de mensagens pelo método RSA, será codificado e decodificado o próprio nome do método, ou seja, RSA.

Antes de codificar esta mensagem, é necessário passar pela etapa de pré-codificação que consiste em associar cada uma das letras a um número conforme as tabelas abaixo:

Tabela 1: Pré-codificação 1

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

Tabela 2: Pré-codificação 2

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

De acordo com a tabela, o R corresponde ao 27, o S corresponde ao 28 e o A corresponde ao 10, depois de pré-codificada, a mensagem se transforma em 272810. Para prosseguir com o método, a primeira etapa na codificação é escolher dois números primos representados pelas letras p e q. Para este exemplo em particular os primos escolhidos são p = 5 e q = 7 que serão importantes para a criação da chave de codificação que será chamada de n, a chave de codificação sempre será o produto dos primos p e q, portanto, para esse caso, a chave de codificação é 35.

A próxima etapa consiste em quebrar em blocos o número gerado pela pré-codificação, por exemplo, 272810 pode se quebrado em 27 - 28 - 10, esta escolha é aleatória, para esse exemplo os blocos têm dois algarismos, mas em geral os blocos podem ser de tamanhos variados, ou seja, um bloco pode conter 3 algarismos, outro com 2, e outro com 1. Há apenas um requisito na hora de formar os blocos, cada um destes blocos não pode ser maior do que a chave de codificação, a razão disto será discutida futuramente.

A codificação se dá a cada bloco por vez por meio da regra:

1. Todos os blocos devem ser elevados a um mesmo número natural representado pela letra lambda $\boldsymbol{\lambda}$;
2. Encontrar o resto da divisão deste número pela chave pública, que para o nosso caso é 35, (esse procedimento equivale a calcular a classe de equivalência no módulo n = 35, do bloco elevado ao expoente $\boldsymbol{\lambda}$)

Em nosso exemplo usaremos $\boldsymbol{\lambda}$ = 7, passemos à codificação:

Bloco 1:

Pelo algoritmo de Euclides temos que:

$$27 = 35.(1) - 8 \Longrightarrow$$

$$27 \equiv (-8) mod 35 \Longrightarrow 27^7 \equiv (-8)^7 mod 35 \Longrightarrow 27 = 35.(1) - 8 \Longrightarrow 27 \equiv (-8) mod 35$$

$$\Longrightarrow 27^7 \equiv (-8)^7 mod 35 \Longrightarrow 27^7 \equiv [(-8)^2]^3 \cdot (-8) mod 35 \Longrightarrow 27^7$$

$$\equiv 64^3 \cdot (-8) mod 35 \Longrightarrow$$

$$27^7 \equiv (-6)^3 \cdot (-8) mod 35 \Longrightarrow 27^7 \equiv (-6)^3 \cdot (-8) mod 35 \Longrightarrow$$

$$27^7 \equiv$$

$$27^7 \equiv 48 \equiv 13(mod35)$$

Bloco 2:

Pelo algoritmo de Euclides temos que $28 = 35.(1) - 7 \Longrightarrow$

$$28^7 \equiv$$

Bloco 3:

$$10 \equiv 10mod35 \Longrightarrow 10^7 \equiv$$

De forma genérica, essas equivalências podem ser representadas através da seguinte expressão $b^{\lambda} \equiv a(modn)$ e sendo assim, 27 - 28 - 10 após a codificação foram transformados em 13 - 7 - 10. Desta forma, a mensagem RSA está codificada.

Para a decodificação da mensagem é necessário uma chave de decodificação, que será formada pelo par de números (n, d), um destes números é o *n* que já foi usado como chave de codificação o outro número será representado pela letra *d* e corresponde ao inverso de $\boldsymbol{\lambda}$ módulo $(p-1)(q-1)$, ou seja:

$$dinversode\lambda[mod(p-1)(q-1)]$$

Assim substituindo cada variável pelo seu respectivo valor, temos:

$$7 \cdot d \equiv 1mod(4.6)$$

$$7 \cdot d \equiv 1mod(24)$$

$$7 \cdot 7 \equiv 1mod(24)$$

$$49 \equiv 1mod(24)$$

Portanto $d = 7$. Encontrado o valor de d, o próximo passo será estabelecer uma regra para a decodificação, tal regra é similar à regra utilizada para codificação e é representada por:

$$a^d \equiv b(modn)$$

Na codificação foi tomado cada bloco b e transformado em um novo bloco a, agora o que será feito é tomar cada um destes blocos representados por ae transformá-lo de volta para o bloco b original. A diferença é que para codificar foi utilizado o expoente $\boldsymbol{\lambda}$ e para decodificar o expoente a ser usado será o d. Assim obtemos os resultados abaixo:

Alguns múltiplos de 35 que podem facilitar a realização dos cálculos:

$$\{35,70,105,140,175,210,\dots\}$$

Para $a = 13$:

$$13^7 \equiv$$

$$\equiv 27(mod35)$$

Portanto, o bloco 13 foi transformado no bloco 27, que corresponde à letra R.

Para $a = 7$:

$$7^7 \equiv$$

$$\equiv (-196) \cdot 7 \equiv 14 \cdot 7 \equiv 28(mod35)$$

Dessa forma, o bloco 7 foi transformado no bloco 28, que corresponde à letra S. Por fim, o cálculo a ser feito será tomar o bloco $a = 10$ e descobrir o resto da divisão de 10^7módulo 35. Mas esse cálculo já foi realizado e resulta em: $10^7 \equiv 10(mod35)$. Este 10 corresponde à letra A de acordo com a tabela, assim a decodificação dos blocos 13 - 7 - 10 é 27 - 28 - 10, que corresponde às letras RSA. Com isso, a mensagem que foi codificada por meio do sistema RSA está decodificada.

O que garante a eficiência do método é a inexistência de uma ferramenta que consiga rapidamente fatorar números muito grandes. Se os primos escolhidos *p* e *q* são “muito grandes”, a chave de codificação fica maior ainda, entendendo-se como “primos grandes” números primos com 200 algarismos o que implicará em uma chave de codificação nada fácil de ser fatorada.

Os métodos existentes e à disposição para a fatoração de números primos levam meses para fatorar números deste tamanho e sem esse processo é impossível descobrir quem são os primos *p* e *q*, mesmo conhecendo o *n*. Outro dado que também será impossível descobrir são o números (*p* - 1) e (*q* - 1) e por consequência o módulo (*p* - 1)(*q* - 1) seguido do valor do número *d* e do expoente que será usado na regra de decodificação: $a^d \equiv b(modn)$. Isso justifica o fato de que o número *n* pode ser um número público, todos podem conhecer, mas os usuários não conseguem decodificar por não conhecerem ou não conseguirem calcular o número *d*.

Uma última observação é que se *p* e *q* são primos muito grandes eles certamente são números ímpares, portanto (*p* - 1) é um número par e (*q* - 1) também

é um número par, logo o produto (p - 1)(q - 1) será um número par. Se o número $\boldsymbol{\lambda}$ escolhido for um número par, ao calcular o inverso de ($\boldsymbol{\lambda}$) módulo (p - 1)(q - 1) acontece um problema pois como $\boldsymbol{\lambda}$ é par assim como o produto (p - 1)(q - 1), não existirá o inverso de $\boldsymbol{\lambda}$. Dessa forma $\boldsymbol{\lambda}$ deve ser escolhido como um número ímpar, mas mesmo assim alguns problemas podem surgir, por exemplo, suponha que $\boldsymbol{\lambda} = 3$.

Após a codificação e decodificação ser realizada, os estudantes deverá tentar reproduzir o processo codificando e decodificando outras palavras, preferencialmente curtas para a motivação podem ser escolhidas pelo professor para facilitar os cálculos.

CONSIDERAÇÕES FINAIS

É indiscutível a importância da criptografia na comunicação para a segurança do que está sendo transmitido, algo que se comprova desde os gregos. A evolução dos métodos de criptografia que ocorreram ao longo do tempo, são resultados do surgimento da computação e da internet. Assim surgiu o método de criptografia RSA que se tornou o sistema criptográfico mais utilizado no mundo.

A teoria dos números fundamenta toda a criptografia RSA, Fermat e Euler contribuíram bastante para o seu desenvolvimento. Sabendo que a segurança do método está ligada ao fato de não existir uma fatoração eficiente, reforça a importância do conhecimento necessário sobre números primos, números inteiros e a matemática residual.

Os tópicos de aritmética como decomposição e uso dos números primos estão relacionados diretamente com o estudo da criptografia RSA. Dessa forma é importante fazer com que os professores busquem um aperfeiçoamento, no intuito de se apropriarem de novos conhecimentos e assim conseguir estimular e desenvolver várias maneiras de abordar alguns conteúdos em matemática.

Espera-se que a realização desta pesquisa possa contribuir para o desenvolvimento de um pensamento exploratório e concreto sobre a teoria dos números, incentivando professores a propor novas atividades em sala de aula e assim estimular o aspecto científico de caráter pesquisador nos alunos.

Entende-se ser possível agregar ao ensino sobre fatoração e algoritmo da divisão a aritmética modular e assim a criptografia se torna um modelo motivador, posto que esteja presente no dia a dia das pessoas por meio das ferramentas digitais.

REFERÊNCIAS

BRASIL. Parâmetros Curriculares Nacionais: Matemática. [S.l.], 1997. Disponível em:<http://portal.mec.gov.br/seb/arquivos/pdf/livro03.pdf>. Acesso em: 04 Jan. de 2021.

COELHO, S. P.; POLCINO MILIES, C**. Números: uma Introdução à Matemática.** São Paulo: Editora da Universidade de São Paulo, 2 000.

FIORENTINI, D.; MIORIN, M. A.. **Uma reflexão sobre o uso de materiais concretos e jogos no ensino de matemática.** Boletim da Sociedade Brasileira de Educação Matemática. São Paulo: SBEM-SP, n.7, p. 1-3, 1990.

FONSECA, Rubens Vilhena. **Percursos investigativos para o trabalho com números primos: uma proposta com o emprego de crivos de primalidade**. UEPA 2014. p. 22 a 27.

FREIRE, Benedito Tadeu Vasconcelos. **Notas de Aula Teoria dos Números.** 2009, p. 22 a 24.

HEFEZ, A**.Elementos de Aritmética.** 2aed. Rio de Janeiro, SBM, 2011

QUEIRÓ, João Filipe. **Teoria dos números.** Departamento de Matemática da Universidade de Coimbra, 2002/2003.

OBMEP - **Olimpíada Brasileira de Matemática das Escolas Públicas**. Disponível em:<www.obmep.org.br>. Acesso em: 04 Jan. de 2021.

RIBENBOIM, Paulo. **Números Primos: Velhos mistérios e novos recordes**. Rio de Janeiro: IMPA, 2012.

SINGH, S.**O Livro dos Códigos**. Rio de Janeiro, Record, 2001.

STALLINGS, W. **Criptografia e Segurança de Redes.** São Paulo, SP: Editora Pearson, 2004. 492 p.