CRIPTOGRAFIA: A EVOLUÇÃO HISTÓRICA E SEU POTENCIAL COMO FERRAMENTA NO ENSINO DE TEORIA DOS NÚMEROS NOS CURSOS DE LICENCIATURA EM MATEMÁTICA

Gabriela Lucheze de Oliveira Lopes [1]; Jaques Silveira Lopes [2]

[1]*Universidade Federal do Rio Grande do Norte, gabriela@ccet.ufrn.br*
[2]*Universidade Federal do Rio Grande do Norte, jaques@ccet.ufrn.br*

Resumo:
Neste artigo buscamos apresentar a criptografia RSA como forma de explorar conceitos da Teoria dos Números na Formação Inicial de Professores de Matemática. A Criptografia está silenciosamente presente na vida de muitas pessoas. A abordagem do tema se justifica na sua vasta aplicação prática, dada a crescente necessidade de enviar dados seguros principalmente pela Internet. Um dos significados para a palavra criptografar é tornar, por meio de normas prescritas num código ou cifra, um texto incompreensível para aqueles que desconhecem esse código. A evolução histórica da prática de criptografar mostra a aplicabilidade da matemática com um cunho sociocultural importantíssimo para o progresso de ideias que desencadearam o funcionamento moderno de alguns criptossistemas. Apresentamos o RSA um sistema de chave pública criado por R. Rivest, A. Shamir e L. Adleman em 1977, esse sistema tem bases teóricas fundamentadas na matemática dos números primos e dos números inteiros em geral. Indicamos o estudo da evolução das práticas criptográficas na história humana e alguns personagens da História da Matemática e da criptografia RSA na componente curricular de Teoria dos Números, presente em algumas estruturas curriculares de cursos de Licenciatura em Matemática no Brasil.
Palavras-chave: Criptografia, Formação de professores de Matemática, Teoria dos Números, Criptografia RSA.

Introdução

A Teoria dos Números, bem como a Álgebra e a Aritmética, como um todo, em muitas das vezes, é vista como uma componente curricular muito abstrata, sofisticada e sem muito espaço para as aplicações e o uso da criatividade e da inovação. Isso acaba gerando uma grande aversão nos alunos, fazendo com que acreditem que é algo difícil, distante da realidade e, muitas vezes, sem utilidades, onde quem aprende ou a compreende é considerado uma pessoa diferente. Para superar essas dificuldades, se faz necessária uma interferência no processo de ensino e aprendizagem de modo a detectar as deficiências e buscar metodologias que possibilitem o acesso a esse conhecimento por todos os estudantes e não somente aqueles que possuem facilidade em aprender.

A apresentação da Teoria dos Números de maneira usual e abstrata é, certamente, um dos motivos para as dificuldades no seu aprendizado. Muitas vezes, são utilizadas apenas

simbologias e manipulações inerentes da linguagem matemática desconectadas de significados para os alunos. De modo que precisamos construir um cenário mais favorável e adequado para a apresentação dessa importante teoria matemática, obviamente de uma maneira que seja acessível ao entendimento dos estudantes. Essa possibilidade didática para a apresentação de conteúdos matemáticos através das aplicações no dia a dia abre inúmeros caminhos para a descoberta de novos conhecimentos que levem o estudante a uma postura de investigação de situações que despertem sua criatividade e o espírito inovador.

Neste artigo buscamos apresentar a criptografia RSA como forma de explorar conceitos da Teoria dos Números, formatada inicialmente por Fermat, na Formação Inicial de Professores de Matemática,

> Conhecido como pai da Teoria dos Números moderna o francês, Pierre de Fermat (1607-1665), nasceu em Toulouse. Escolheu o direito como profissão e perseguiu a Matemática apenas como um amador. Desenvolveu a análise algébrica, com base nas obras de Viète e desenvolveu importantes trabalhos na geometria analítica e óptica. É considerado fundador da teoria dos números moderna seguindo a tradição diofantina. Seus dois maiores desafios na Matemática, em 1657-8, levaram a extensa correspondência com Wallis, Brouncker e Frenicle. Correspondências estas que podem ser encontradas em *Commercium epistolicum de quaestionibus quibusdam mathematicis nuper habitum* de 1658. (LOPES, 2016, p. 100, grifo da autora).

A Criptografia está silenciosamente presente na vida de muitas pessoas. A abordagem deste tema se mostra sobremaneira importante dada a sua vasta aplicação prática, além de uma crescente necessidade de enviar dados seguros de maneira segura, principalmente pela Internet.

Um dos significados para a palavra criptografar é tornar, por meio de normas prescritas num código ou cifra, um texto incompreensível para aqueles que desconhecem esse código. A evolução histórica da prática de criptografar mostra a aplicabilidade da matemática com um cunho sociocultural importantíssimo para o progresso de ideias que desencadearam o funcionamento moderno de alguns criptossistemas. Apresentamos o RSA um sistema de chave pública criado por R. Rivest, A. Shamir e L. Adleman em 1977, esse sistema tem bases teóricas fundamentadas na matemática dos números primos e dos números inteiros em geral. Indicamos o estudo da evolução das práticas criptográficas na história humana e alguns personagens da História da Matemática e da criptografia RSA na componente curricular de Teoria dos Números, presente em algumas estruturas curriculares de cursos de Licenciatura em Matemática no Brasil.

Metodologia

Apresentamos, de maneira destacada, fatos históricos relacionados à Teoria dos Números, em particular da Criptografia. Isso é feito, porque acreditamos no grande potencial pedagógico da utilização da história da Matemática e de seu desenvolvimento, possibilitando o enriquecimento das aulas, discutindo com os alunos os aspectos sociais e culturais que sobressaíram daquele recorte histórico estudado, estabelecendo assim uma integralização da Matemática, em particular da Criptografia, ao contexto social e cultural de certo período histórico. Esse pensamento é consonante ao ponto de vista de Valdés (2006), que assegura que a história deveria ser um potente auxiliar para alcançar o objetivo de demarcar temporalmente e espacialmente as grandes ideias, problemas, junto com a sua motivação, os seus precedentes; além de contribuir para desmistificar a visão individualista dada aos matemáticos que mudaram o domínio da Matemática acrescentando suas ideias criativas, declarados como gênios pela maioria das pessoas, ignorando dessa forma o papel exercido pelo trabalho coletivo de gerações e de grupos de matemáticos.

Segundo Miorim e Miguel (2011) a história da matemática contribui no ensino da matemática ao mostrar: A matemática como uma criação humana; As razões pelas quais as pessoas fazem matemática; As necessidades práticas, econômicas e físicas que servem de estímulo ao desenvolvimento das ideias matemáticas; As conexões existentes entre matemática e filosofia, matemática e religião, matemática e lógica, etc.; A curiosidade estritamente intelectual que pode levar a generalização e extensão de ideias e teorias; As percepções que os matemáticos têm do próprio objeto da matemática, as quais mudam e se desenvolvem ao longo do tempo; A natureza de uma estrutura, de uma axiomatização e de uma prova.

Mais ainda, devemos valorizar as histórias concernentes aos aspectos matemáticos em seu processo de criação, reinvenção e organização lógica, firmados no tempo e no espaço com a finalidade de sistematizar soluções de problemas de ordem sociocultural, científica e tecnológica, em todos os tempos e lugares. Corroboramos com Chaquiam (2015) no sentido em que destacamos que a cultura matemática historicamente instituída que tem um potencial enriquecedor e viável para esclarecer os estudantes sobre os modos como a matemática se desenvolveu temporal e espacialmente.

Para que essa proposta por meio dessa abordagem de conteúdos de Matemática, que utilizem a história da Matemática como ferramenta metodológica se materialize, devemos

admitir que o professor tenha bom conhecimento da Matemática ensinada, em particular da Teoria dos Números e da Teoria da Criptografia. De modo que o professor possa visualizar e até planejar novas possibilidades sobre os temas abordados. Concordamos, assim, com a visão de que

> A matemática, como qualquer área do conhecimento humano, tem seu desenrolar evolutivo capaz de caracterizá-la como uma ciência que também se desenvolve a partir da sua própria história. Desse modo podemos buscar nessa história fatos, descobertas e evoluções que nos mostrem o caráter criativo do homem quando se dispõe a elaborar e disseminar a ciência matemática no seu meio sócio-cultural. Cabe-nos, entretanto, o cuidado de saber buscar na história da matemática a medida certa para nos tornarmos capazes de adquirir o espírito presente nesse conhecimento. (MENDES, 2001 p.18)

Nesse sentido, como já salientamos anteriormente, os cursos de formação de professores de Matemática devem oferecer aos seus estudantes ambientes e métodos que levem a uma aprendizagem consistente da teoria Matemática em discussão.

Discussão e Resultados

Em grego, *cryptos* significa secreto, oculto, e *graphia*, escrita. Criptografia é, portanto, a arte da escrita secreta, dos códigos secretos. A criptografia estuda os métodos para codificar uma mensagem sem que haja o comprometimento do sigilo, isto é, de modo que só seu destinatário legítimo consiga interpretá-la. ara tornar mensagem incompreensível, as informações, sejam elas textos, números ou qualquer outra forma de dados, são trocados ou misturados, ou ambos, de acordo com um protocolo específico, estabelecido previamente pelos transmissores e receptores da mensagem. Assim, o receptor pode reverter o protocolo e tornar a mensagem compreensível.

A criptografia nasceu da necessidade que tinham os reis, rainhas e generais, desde as épocas mais remotas da humanidade, de uma comunicação eficiente para governar seus países e comandar seus exércitos, e, ao mesmo tempo, de garantir o segredo de suas mensagens, caso fossem interceptadas por mãos erradas. O primeiro exemplo de um código secreto é também o mais simples, e foi criado por Julio César, antigo Imperador de Roma, em torno do ano 60 a.C., para comunicar-se com suas legiões em combate pela Europa.

Atualmente, com o crescimento das transações comerciais via internet e o surgimento das criptomoedas, a criptografia é a principal tecnologia dos sistemas de segurança eletrônica, mas talvez seja tão antiga como a própria escrita.

A criptografia pode servir de motivação ou despertar interesse dos jovens pela matemática como este episódio da História da Matemática. A Criptografia, como campo de interesse da Matemática, sempre esteve na pauta de interesse de grandes matemáticos, John Wallis (1616-1703) se interessou por matemática após ter contato com um problema de criptografia apresentado por seu irmão. No Natal de 1631, na casa de sua mãe em Ashord, Wallis encontra o seu irmão mais novo e, movido por sua curiosidade, ele aprende "em cerca de 8 ou 12 dias" a "escrever em cifras" e a operações comuns no comércio, 'adição, subtração, multiplicação, divisão e regra de três". Em sua autobiografia Wallis declara que foi seu primeiro contato com a Matemática. Todavia,

> A Matemática que Wallis descobriu não tinha nenhuma geometria, era só a aritmética e a álgebra rudimentares de contabilidade. Não havia teoremas nem provas nesse tipo de Matemática e nenhum sopro das grandiosas afirmações filosóficas enunciadas em nome da geometria euclidiana (ALEXANDER, 2016, p. 262).

Todo sistema criptográfico necessita de dois elementos indispensáveis: um algoritmo e uma chave, que especificam os detalhes exatos de uma codificação em particular. O algoritmo é o procedimento utilizado para codificar a mensagem e, neste caso, consiste em substituir cada letra do alfabeto original por outra do alfabeto cifrado. A chave define o alfabeto cifrado exato que será usado em uma codificação em particular. O Princípio de Kerckhoff, assim definido em 1883 pelo linguista holandês Auguste Kerckhoff em seu livro *La Cryptographie Militaire* :A segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo (chave de codificação). A segurança depende apenas de se manter em segredo a chave (de decodificação).

Os sistemas criptográficos podem ser classificados de duas maneiras: simétricos e assimétricos.

Em um sistema simétrico, a chave de codificação é igual à chave de decodificação, e, obviamente, tem que ser mantida em segredo. Neste sistema, a decodificação é o processo inverso da codificação. O código secreto de César é um exemplo de criptossistema simétrico. Este sistema tem a inconveniente característica da facilidade de descobrimento de sua chave, mas pode ser utilizado em tipos de comunicação em que ambas as partes se confiam mutuamente.

Em um sistema assimétrico, a chave de codificação é diferente da chave de decodificação, e é inviável descobrir uma a partir da outra. Neste tipo de criptografia, a chave

de decodificação deve ser preservada em segredo, mas a de codificação pode ser tornada pública, sem comprometer o sistema. Por isso, os criptossistemas assimétricos também são chamados de *criptossistemas de chave pública*. Aqui, saber criptografar não implica saber decriptografar, pois são processos distintos.

Uma evolução histórica da Criptografia, começa com os métodos de Substituição Simples, 600 a 500 a.C., *no Livro de Jeremias e as Cifras Hebraicas*. Na Tabela 1 apresentamos uma cronologia destacando alguns personagens, conteúdos da Teoria dos números e tipos d criptografia:

Tabela 1- Evolução Histórica da Criptografia

Período	Personagens, conteúdo matemático ou tipo de criptografia
487 a.C.	Tucídides e o Bastão de Licurgo, cifra de transposição.
± 300 a.C.	Os Elementos de Euclideas , teoria dos números e números primos.
276 a 194 a.C.	O Crivo de Erastótenes, números primos.
204 a 122 a.C.	O Código de Políbio, substituição poligrâmica.
50 a.C.	O Código de César, substituição simples.
79 d.C.	A Fórmula Sator ou Quadrado Latino.
801 a 873	al-Kindi e a Criptanálise.
1119 a 1311	Templários, substituição simples por símbolos.
1466	Leon Battista Alberti: inventor da substituição polialfabética.
1518	Johannes Trithemius, esteganografia.
1533	Cifra de Pig Pen: substituição simples por símbolos.
1550	Girolamo Cardano, esteganografia e substituição com auto-chave.
1553	Giovanni Battista Bellaso, substituição polialfabética com palavra-chave.
1558	Philibert Babou, substituição homofônica.
1563	Giambattista Della Porta, substituição polialfabética com palavra-chave.
1586	Blaise de Vigenère, substituição polialfabética com palavra-chave.
1854	Charles Babbage e as Máquinas de Diferenças Cifra Playfair.
1917	William F. Friedman considerado o pai da *criptoanálise norte-americana*.
1920	A cifra de Bazeries: uma recifragem com métodos clássicos.
1974	A cifra de bloco DES - O NBS publica o padrão dos EUA.
1977	Método RSA: criado por R. Rivest, A. Shamir e L. Adleman

Fonte: Elaborado pelos autores

É deste ponto histórico retomamos nossa discussão sobre o método de Criptografia utilizado como ferramenta pedagógica, a saber o RSA. Como dissemos anteriormente o RSA é um sistema de chave pública criado por R. Rivest, A. Shamir e L. Adleman. Esse sistema tem bases teóricas fundamentadas na matemática dos números primos e dos números inteiros em geral. E por ter essa base matemática suportada na aritmética dos números primos é que este método foi escolhido para ser apresentado como uma importante aplicação de Teoria dos Números e motivar seu aprendizado.

A base matemática do criptossistema RSA se fundamenta nos seguintes conteúdos de Teoria dos Números: Indução matemática; Divisibilidade e propriedades; Algoritmo da divisão euclidiana; Maximo divisor comum; Números primos; Fatoração em primos; Crivo de Erastótesnes; Números de Fermat; Números de Mersene; Congruências; Função de Euler; Teorema de Fermat; Teorema Chinês do Resto.

O sistema RSA foi o primeiro criptossistema de chave pública e ainda é um dos mais importante, tendo sido criado em 1977 por três pesquisadores do Laboratório de Ciência de Computação do Massachussets Institute of Technology (M.I.T.). As letras RSA correspondem às iniciais dos sobrenomes de seus criadores : Ronald Rivest, Adi Shamir e Leonard Adleman. É o criptossistema mais usado em aplicações comerciais (aproximadamente 95% dos sites de comércio eletrônico o utilizam). O RSA tem suas bases teóricas fundadas na matemática dos números primos e dos números inteiros em geral, utilizando-se de um ramo da Matemática chamado de Teoria dos Números. Explicaremos detalhadamente como foi desenvolvido o referido criptossistema, analisando matematicamente cada passo do seu funcionamento e o porquê de sua eficiência.

Por razões didáticas e práticas e para facilitar o entendimento, o método de criptografia RSA foi dividido em 3 partes principais : etapa de pré-codificação, etapa de codificação e, por fim, etapa de decodificação. Vamos detalhar, baseados em Coutinho (1997) cada uma destas etapas, apontando os conteúdos matemáticos envolvidos:

1) ETAPA DE PRÉ-CODIFICAÇÃO**:** Para utilizar o método de criptografia RSA, primeiro precisamos converter a mensagem em uma seqüência de números. Para efeito de simplificação não faremos distinção entre maiúsculas e minúsculas e nem consideraremos sinais de pontuação. Para esta conversão utiliza-se a Tabela 2:

Tabela 2 – Pré-codificação no sistema RSA

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

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

Fonte: Elaborado pelos autores

Quando houver espaço entre duas palavras usamos o número 99. Como exemplo, a palavra *Matemática* seria convertida no número 22102914221029181210.

2) ETAPA DE CODIFICAÇÃO: Feita a pré-codificação, obtemos uma sequência de números. Separamos este número em uma sequência de blocos menores, de forma que o número formado por cada bloco seja menor que $n = p.q$, onde p e q são números primos distintos e também escolhemos um número e tal que $MDC(n,e) = 1$. Denotemos esses blocos por b_i, onde $i = 1, 2, 3, \ldots$. O bloco codificado, que chamaremos de $C(b_i)$, é o resto da divisão b_i^e por n, ou $C(b_i)$ é a menor solução positiva da congruência: $b_i^e \equiv C(b_i)(\mathrm{mod}\, n)$. A partir daqui os blocos codificados serão denotados por x_i , ou seja, $x_i = C(b_i)$, para $i = 1, 2, 3, ..., k$.

No caso particular da palavra *matemática,* escolhemos o número n=7.11=77 e $e = 3$ sua pré-codificação deu o número 22102914221029181210. Separamos este número em uma sequência de blocos menores, de forma que o número formado por cada bloco seja menor que n=77. Denotamos esses blocos por b_i, onde i = 1; 2; :::; k. O número encontrado na pré-codificação 22102914221029181210, pode ser assim subdividido 22-10-29-14-22-10-29-18-12-10. Particularmente temos b_1=22, b_2=10, b_3=29, ... Para encontrar os blocos codificados $C(b_i)$, que é o resto da divisão b_i^e por n, temos que resolver as seguintes congruências:

$$22^3 \equiv C(b_1)(\mathrm{mod}\, 77) \Rightarrow 10648 \equiv 22(\mathrm{mod}\, 77) \Rightarrow C(b_1) = 22$$

$$10^3 \equiv C(b_2)(\mathrm{mod}\, 77) \Rightarrow 1000 \equiv 76(\mathrm{mod}\, 77) \Rightarrow C(b_2) = 76$$

$$29^3 \equiv C(b_2)(\mathrm{mod}\, 77) \Rightarrow 24389 \equiv 57(\mathrm{mod}\, 77) \Rightarrow C(b_3) = 57$$

E assim por diante.

3) ETAPA DE DECODIFICAÇÃO: Para decodificar a mensagem é preciso encontrar uma relação, denotada por $D(x_i)$, tal que:

$D(x_i) \equiv b_i (\mathrm{mod}\, n)$. De modo que, se b_i é um inteiro, relativamente primo com n, o Teorema de Euler nos dá que $b_i^{\phi(n)} \equiv 1(\mathrm{mod}\, n)$. Como p e q são primos, segue, da função de de Euler, que $\phi(p) = p-1$ e $\phi(q) = q-1$. Além disso, $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$. Para decifrar a mensagem é necessário encontrar um inteiro d tal que $e.d \equiv 1(\mathrm{mod}\, \phi(n))$, o que implica em $e.d \equiv 1(\mathrm{mod}(p-1)(q-1))$ que, pelo Teorema de Euler, tem-se $d \equiv e^{\phi((p-1)(q-1))-1}(\mathrm{mod}(p-1)(q-1))$. Assim, de $e.d \equiv 1(\mathrm{mod}\, \phi(n))$ concluímos que existe um inteiro t tal que $e.d \equiv t.\phi(n)+1$. Logo, $b_i \equiv b_i.1 \equiv b_i(t)^t \equiv b_i(b_i^{\phi(n)})^t \equiv b_i^{t.\phi(n)+1}(\mathrm{mod}\, n)$ e $b_i^{t.\phi(n)+1} \equiv b_i^{ed} \equiv (b_i^e)^d \equiv (C(b_i))^d \equiv x_i^d (\mathrm{mod}\, n)$. Portanto $D(x_i) \equiv x_i^d (\mathrm{mod}\, n)$. Observemos que $D(x_i)$ é a relação inversa de $C(b_i)$.

Vale ressaltar que os parâmetros do sistema RSA são dois números primos, p e q, muito grandes (da ordem de 10^{100}) e com uma grande diferença numérica entre si. Estes números são a base da criptografia RSA. Mas, para escolhermos números primos tão grandes, temos que nos certificar da existência destes números, por maior que eles sejam. Para isso, teremos que provar o seguinte resultado: Existem infinitos números primos, teorema que pode ser demonstrado utilizando a indução matemática e fatoração em primos.

Agora podemos escolher números primos tão grandes quanto se queira. Mas como saber se números tão grandes, de mais de 100 algarismos, são de fato primos? É praticamente impossível dividir números desta ordem de grandeza por todos os primos menores do que ele como indicado pelo Crivo de Erastótenes. Para contornar esta dificuldade, ao longo da história foram desenvolvidos vários algoritmos e fórmulas para verificar a primalidade de um número.

Os algoritmos de primalidade, quanto ao tempo necessário para se computar o resultado, que é o de verificar se um dado número é primo ou não, podem ser classificados em algoritmos de tempo exponencial e algoritmos de tempo polinomial. Nos algoritmos de tempo exponencial o tempo de processamento para obter a solução cresce exponencialmente quanto mais cresce o número. Este tipo de algoritmo não é adequado para números muito grandes, como é o caso dos parâmetros p e q do RSA. Já nos algoritmos de tempo polinomial, temos um tempo de resposta razoável, frente ao tamanho do número. A seguir, vamos indicar algumas supostas fórmulas, encontradas na História da Matemática, para se achar números primos.

Marin Mersenne foi um frade e matemático amador do século XVII. Ele afirmou, mas

sem apresentar nenhuma justificativa, que os números da forma $M(n) = 2^n - 1$, chamados de NÚMEROS DE MERSENNE, seriam primos para n valendo 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257, e compostos para todos os outros 44 valores primos de n menores que 257. Posteriormente, alguns erros foram descobertos nesta afirmação: a lista omite os primos M(61), M(89) e M(107), e incluiu os compostos M(67) e M(257). Apesar destas falhas, os números de Mersenne são uma rica fonte de números primos. Como exemplo disto, temos o maior primo conhecido atualmente que é o 50º primo de Mersene descoberto pelo grupo de pesquisa *Great Internet Mersenne Prime Search* (GIMPS, 2018) em 26 de dezembro de 2017. Esse primo tem 23.249.425 dígitos, e é o maior número primo conhecido pela humanidade. Esse é enorme, com dígiots suficientes para encher uma prateleira inteira de livros totalizando 9.000 páginas.

O francês Pierre de Fermat, também no século XVII, em uma de suas correspondências a outros matemáticos da época, enumerou os números da forma $F(n) = 2^{2^n} + 1$, para n variando de 0 a 6, e afirmou que estes números eram primos. Estes números são: 3, 5, 17, 257, 65.537, 4.294.967.297 e 18.446.744.073.709.551.617. Hoje, sabe-se que apenas os quatro primeiros NÚMEROS DE FERMAT são primos, e estima-se que não exista nenhum outro número de Fermat que seja primo.

Desta forma, mostramos alguns dos diversos conteúdos de Teoria dos Números que emergem do estudo de Criptografia.

Conclusões

Neste trabalho formamos a ideia de que os códigos secretos têm curto prazo de validade, pois sua criação sempre dá origem a uma força oposta que visa quebrá-los. Normalmente essa força é constituída por pessoas, países ou instituições que estão interessados na informação escondida pelo código. Essa luta entre criptoanalistas, como denominamos esses cientistas que estudam as diferentes formas de criptogramas, faz com que os métodos devam ser melhorados a cada instante. É importante salientar que a criptologia é uma ciência em constante evolução, pois não há como garantir por quanto tempo um método criptográfico será seguro. No trabalho, citamos que o RSA é um modelo de criptograma usado para manter a segurança das pessoas que realizam transações comerciais pela internet e

falamos também sobre sua segurança. Convém ressaltar, porém que embora o método seja seguro, só a criptografia dados não garante que uma pessoa não possa ter seus dados expostos na internet, não por falha na cifragem dos mesmos e sim por descuido da própria pessoa. Com esse trabalho procuramos ressaltar que o método RSA tem uma importância significativa para a matemática, pois deu uma importante aplicação à Teoria dos Números, que possuía, antes dele, pouca aplicação prática. Com tantas possibilidades, a criptografia deve ser cada vez mais trabalhada e estimulada em sala de aula nas escolas, onde pode aparecer com resolução de desafios colocados aos alunos.

Referências

ALEXANDER, *A.* Infinitesimal: a teoria Matemática que revolucionou o mundo. Tradução George Shlesinger, 1. ed, Rio de Janeiro: Editora Zahar, 2016.

CHAQUIAM, M. História da Matemática em sala de aula: proposta para integração aos conteúdos matemáticos. São Paulo: Livraria da Física, 2015.

COUTINHO, S. C. (1997) Números Inteiros e Criptografia RSA, IMPA, Rio de Janeiro.

GIMPS, Great Internet Mersenne Prime Search. Disponível em <https://www.mersenne.org/> Acesso 05 de set.2018.

MENDES, I. A. O Uso da História no Ensino da Matemática: reflexões teóricas e experiências**.** Belém: EDUEPA, 2001. 90 p.

MENDES, I.A; FOSSA, J.A;VALDES,J.E.N. A história como um agente de cognição na educação matemática. Porto Alegre: Sulina, 2006.182 p.

MIGUEL, A; MIORIM, M. A. História na Educação Matemática: propostas e desafios. 2. ed. Belo Horizonte: autentica editora, 2011. 208 p.