V SEMANA UNIVERSITÁRIA DA URCA
XXIII Semana de Iniciação Científica
07 a 11 de Dezembro de 2020
Tema: "Os impactos e desafios da pandemia COVID no ensino, pesquisa e extensão"
ISSN 1983-8174

CRIPTOGRAFIA RSA: UMA APLICAÇÃO DA TEORIA DOS NÚMEROS

Antonia Erineide Cavalcante[1], José Augusto Pereira Nogueira[2]

Resumo: Esse trabalho é uma pesquisa bibliográfica sobre a Matemática Aplicada, com ênfase em alguns conceitos fundamentais da Teoria dos Números, aplicáveis através dos métodos Criptográficos e essenciais para abordagem do tema, a Criptografia RSA. Antes do desenvolvimento expressivo da Criptografia, a Teoria dos Números era considerada uma área da matemática sem aplicações práticas. Objetivamos com esse estudo um entendimento do uso da Matemática no cotidiano das pessoas, buscando a compreensão e explicação dos mesmos de maneira clara e concreta. Para o desenvolviimento do trabalho pesquisamos sobre o assunto em materiais científicos como artigos, monografias, dissertações e livros. A Criptografia RSA é um dos métodos de encriptação mais seguros e cofiavéis para o sigilo de mensagens, dados bancários, por operar com números primos e fatoração tornando complexa a decodificação. Sem dúvida esse estudo tem uma relevância importante para toda comunidade acadêmica e de maneira geral para todos que o tenha acesso.

Palavras-chave: Criptografia. Criptografia RSA. Matemática Aplicada. Teoria dos Números.

1. Introdução

Com uso frequente da tecnologia e em decorrência disso uma maior necessidade de sigilo de informações pessoais, a Criptografia, ramo antigo da Matemática, vem sendo mais usada no cotidiano, muitas vezes parece imperceptível, pelas pessoas. Criptografia é a "escrita oculta". De origem grega "*kryptós*" quer dizer "esconder", "*gráphein*", significa "escrever". A Criptografia RSA é um dos métodos criptográficos mais conhecidos e seguros hoje em dia.

Foi criada pelos matemáticos Whitfield Diffie e Martin Hellman com o intuito de codificar uma mensagem, computacionalmente, uma função f(n) para ser calculada (codificada), onde fosse praticamente impossível calcular (decodificar) sua inversa.

A Teoria dos Números é a área da Matemática que proporciona aplicar e explicar os procedimentos desse método, através de conceitos básicos como: divisibilidade, Máximo Divisor Comum (MDC), números primos, entre outros introduzidos nesse trabalho.

É no processo, codificação e decodificação, onde o essencial é assegurar o sigilo das mensagens enviadas pelo emissor para seu receptor, que a Matemática através da Teoria dos Números ressalta sua importância e aplicabilidade de maneira real.

---

1 Universidade Regional do Cariri, email: eryneyde.cavalcante@urca.br
2 Universidade Regional do Cariri, email: augusto.nogueira@urca.br

ISSN 1983-8174

2. Objetivo

Objetivamos com esse estudo a compreensão geral e clara sobre a Criptografia e, principalmente, a Criptografia RSA, sua segurança, funcionamento até chegar em suas principais implicações de forma concreta.

3. Metodologia

Estudo desenvolvido a partir de artigos, dissertações, monografias que abordam os fundamentos da Teoria dos Números e aplicações da Criptografia. São alguns conceitos de efeitos diretos nos métodos criptográficos, por isso não teremos demonstrações de tais conceitos.

Divisibilidade: dados dois inteiros ($\mathbb{Z}$) d, a, $a \neq 0$, dizemos que a divide d, e escrevemos $a \mid d$, se existir $n \in \mathbb{Z}$ tal que $d = a \cdot n$ ou $a \cdot n = d$, ou seja, d um múltiplo de a.

Quando a divide d, denotamos $a \mid d$. Caso contrário, a não divide d, e escrevemos $a \nmid d$.

Teorema 1 (Algoritmo da Divisão): dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem inteiros únicos, tais que $a = b \cdot q + r$ e $0 \leq r < |b|$. ($r = 0$ se, e somente se, $b \mid a$).

Chamamos q de quociente e r de resto da divisão.

Lema: Sejam $a, b, c, d \in \mathbb{Z}$. Temos

(i) (d divide) Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes $x, y \in \mathbb{Z}$.
(ii) (Limitação) Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.
(iii) (Transividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Máximo Divisor Comum: D(n) é denotado como conjunto dos divisores de n. Dados dois inteiros a, b com a e b não nulos, D(a, b) é o conjunto de todos os divisores comuns de a e b. Chama-se máximo divisor comum ao maior divisor comum de a e b, indicado por mdc(a, b).

$$\text{mdc}(a, b) = \max D(a, b)$$

D(a, b) é finito, assim sempre possui um maior elemento, como $a \neq 0$ ou $b \neq 0$, mdc(a, b) ≥ 1.

Números Primos: é chamado de primo um inteiro $p > 1$ com exatamente dois divisores positivos, 1 e p.

Proposição 1. Seja p um número primo e a e b números inteiros.

ISSN 1983-8174

(i) Se $p \nmid a$, então mdc (p, a) = 1
(ii) Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Congruências: seja $m \neq 0$ um inteiro fixo. Dizemos que a é congruente a b módulo m, sendo a e b dois inteiros, se m divide $a - b$. Escrevemos a ≡ b (mod m)

$$a \equiv b\ (mod\ m) \Leftrightarrow m \mid a - b \Leftrightarrow \exists\ q\ \in\ \mathbb{Z}\ tal\ que\ a - b = m\ \cdot q \Leftrightarrow a = m\ \cdot q + b$$

portanto, a é côngruo a b módulo m, se, e somente se, b é o resto da divisão de a por m.

Teorema 2 (Pequeno Teorema de Fermat): Sejam p um número primo e a um número inteiro tal que $p \nmid a$. Então

$$a^{p-1} \equiv 1(mod\ p).$$

Função fi (φ) de Euler: A função φ de Euler: $\mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ é denotada por $\varphi(m)$, definida como sendo o número de inteiros positivos menores ou iguais a m que são relativamente primos com m.

Teorema 3 (Teorema de Euler): Sejam m, $a \in \mathbb{Z}_+$ com $m > 1$ e mdc(a, m) = 1. Então

$$a^{\varphi(m)} \equiv 1(mod\ m)$$

4. Resultados

Criptografia RSA: o método criptográfico RSA é dos primeiros sistemas de chave pública que contém em seu processo duas chaves de segurança, uma pública e uma privada. A pública (encriptação) pode ser conhecida por qualquer pessoa além do remetente e do destinatário. A chave privada (decriptação) só o destinatário conhece. Essencial para sigilo de mensagens, dados bancários, etc. Para usar esse método são necessários três processos: pré-codificação, codificação e decodificação. Primeiro passo é preciso de dois números primos, p e q. Para codificação faz-se o produto de p e q para conhecer m. O último passo é saber o valor de p e q para conseguir a decodificação da mensagem.

Pré-codificação: é o processo usado para converter uma mensagem normal em mensagem codificada. É o processo de transformar as 26 letras do alfabeto em números. Esses números precisam ser de dois dígitos para não gerarem ambiguidades, como mostra a tabela 1.

Tabela 1 – Transformação das letras em números

A	B	C	D	E	F	G	H	I	J	K	L	M

ISSN 1983-8174

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: Adaptado de Oliveira (2013, p. 36)

Quando a mensagem possui mais de uma palavra no espaço entre uma e outra é usado o número 99.

Exemplo: Realizar os processos de encriptação e decriptação da mensagem "RSA" através do método criptográfico RSA.

Pré-codificação. Observando a Tabela 1 temos: 272810. Considerando os primos distintos $p = 5$ *e* $q = 7$, obtemos a chave de codificação: $m = p \cdot q = 35$. Separando a mensagem em blocos de dois números, temos: 27 – 28 – 10.

Codificação. Utilizando a congruência $b^e \equiv a(mod\ m)$, com $e = 7$, obedecendo a função φ de Euler, e obtém esse valor por ser o menor número inteiro primo com 35, codificaremos cada bloco.

$$27^7 \equiv 13(mod\ 35);\ 28^7 \equiv 7(mod\ 35);\ 10^7 \equiv 10(mod\ 35)$$

Decodificação. $a^d \equiv b(mod\ m)$ onde d é o inverso de e $[mod\ (p-1)(q-1)]$

Logo, $7d \equiv 1\ [mod(4 \cdot 6)] \Rightarrow 7d \equiv 1(mod\ 24) \Rightarrow d = 7$.

Agora decodificando os restos da codificação: 13 – 7 –10.

$$13^7 \equiv 27(mod\ 35);\ 7^7 \equiv 28(mod\ 35);\ 10^7 \equiv 10(mod\ 35)$$

Portanto, decodificamos a mensagem: $27 \rightarrow R \quad 28 \rightarrow S \quad 10 \rightarrow A$.

Assim como essa, milhões de mensagens são codificadas todos os dias, utilizadas em todo o mundo de forma sigilosa com auxilio de sistemas computacionais e apresentam um grau de complexidade maior que essa exemplificada.

O exemplo demonstrado acima é bem simples com o objetivo de facilitar o entendimento do leitor, mas vale ressaltar que no cotidiano, principalmente pelo uso tecnológico, os números primos distintos *p* e *q* são muito grandes com milhares de algoritmos, por esse motivo a chave de codificação (*m*) que é pública se torna maior que esses parâmetros, como também são conhecidos. Tornando impossível a fatoração de *m* e, consequentemente, a decodificação da mensagem. Permitindo assim que a transmissão de informações aconteça de forma segura.

ISSN 1983-8174

5. Conclusão

De maneira sucinta concluímos que a Teoria dos Números oportuniza através de seus conceitos básicos essenciais aplicações criptográficas e que a Matemática está não só presente, mas é imprescindível em funções básicas do dia a dia de todas as pessoas.

Esperamos que esse estudo seja fonte instigante para conhecimento da Teoria dos Números, da Criptografia, principalmente, da Criptografia RSA que é um ramo da Matemática em constante desenvolvimento de aplicações práticas, tecnologicas, que traz a tona um conhecimento matemático em construção, na busca de novas descobertas e práticas.

6. Agradecimentos

Agradecemos a URCA e aos recursos de financiamento do FECOP pela concessão da bolsa do Programa Institucional de Bolsas de Iniciação Científica (PIBIC).

7. Referências

BARBOSA, H. F. **Teoria dos Números e Criptografia.** TCC (Departamento de Matemática) - Universidade Federal de São Carlos, São Carlos, 2008. Disponível em: < https://www.dm.ufscar.br/~ptlini/TCC_Henrique_Favarom_Barbosa.pdf>. Acesso em: 14 de nov. 2020.

GALDINO, U. A. **Teoria dos Números e Criptografia com Aplicações Básicas.** TCC (Mestrado Profissional - PROFMAT) – Universidade Estadual da Paraíba, Campina Grande, 2014. Disponível em: <http://tede.bc.uepb.edu.br/jspui/bitstream/tede/2266/5/PDF%20-%20Uelder%20Alves%20Galdino.pdf>. Acesso em: 14 nov. 2020.

MOREIRA, C. G. T. de A.; MARTÍNEZ F. E. B.; SALDANHA, N. C. **Tópicos de teoria dos números**. 1. ed. Rio de Janeiro: SBM, 2012.

OLIVEIRA, M. C. **Aritmética:** criptografia e outras aplicações de congruências. TCC (Mestrado em Ciências Exatas e Tecnologia: PROFMAT) – Universidade Federal de Mato Grosso do Sul, Campo Grande, 2013. Disponível em: <https://repositorio.ufms.br:8443/jspui/handle/123456789/2160>. Acesso em: 14 nov. 2020.