Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 3, N. 1, 2015.
Trabalho apresentado no XXXV CNMAC, Natal-RN, 2014.

Congruência Modular aplicada à Criptografia

Djair P. dos Santos **Lindinês C. da Silva**
Fernando V. Costa Júnior **Elthon A. da S. Oliveira**
Universidade Federal de Alagoas, UFAL, 57309-005, Arapiraca, AL
E-mail: djairpsc@hotmail.com, lindinescoleta@hotmail.com,
fernando.math@hotmail.com, elthon@arapiraca.ufal.br.

RESUMO

Nos meios eletrônicos e internet existem várias informações que devem ser mantidas em sigilo, as quais somente o emissor e o destinatário podem saber. Um meio de garantir o sigilo da informação é a criptografia, palavra que vem do grego kryptós = "secreto" e gráphein = "escrita", que é o estudo das técnicas de codificação/decodificação de informações. A criptografia busca a melhor forma de transformar dados em material dificilmente decifrável através de processos puramente matemáticos. Uma das ferramentas mais comuns é o uso da Matemática Discreta para, através da Congruência Modular, trabalhar sobre um código numérico onde apenas quem tem a chave de descriptografar consegue ler a mensagem (Cf. [1]). Este trabalho objetiva mostrar a importância da criptografia, e como a Criptografia RSA funciona a partir da aplicação da Congruência Modular, exibindo sua construção e funcionamento.

Definição 1: Definimos a *Função de Euler* como sendo a função $\varphi : \mathbb{N} \to \mathbb{N}$, onde $\varphi(n) = \sharp\{k \in \mathbb{N}^* | k \leq n \wedge mdc(k,n) = 1\}$.

Definição 2: Sejam $a, b \in \mathbb{Z}$ e n um inteiro positivo. Dizemos que a *é congruente a* b *módulo* n, e escrevemos $a \equiv b \ \ (mod\ n)$, se, e somente se, $a - b$ é múltiplo de n.

Estas definições nos serão úteis para a construção da Criptografia RSA. Esta envolve um par de chaves: uma pública (que pode ser conhecida por todos) e uma privada (que deve ser mantida em sigilo). Toda mensagem cifrada usando uma chave pública só pode ser decifrada usando a respectiva privada.

Escolhe-se dois números primos gigantescos, p e q, preferencialmente com mais de cem dígitos, e define-se $N = p.q$. Cada pessoa que utiliza o sistema escolhe um $k \in \mathbb{N}$, tal que $mdc(k, \varphi(N))= 1$, e então obtém-se a chave pública, que será (N, k), usada da seguinte forma:

$$\text{(texto codificado)} \equiv \text{(texto original)}^k \ \ (mod\ N)$$

Para obter a chave privada (N, t), que decodificará a mensagem, é necessário resolver a congruência $kt \equiv 1 \ \ (mod\ \varphi(N))$. Tal chave é usada da seguinte maneira:

$$\text{(texto original)} \equiv \text{(texto codificado)}^t \ \ (mod\ N)$$

Como apenas o emissor e o destinatário da mensagem tem acesso aos números p e q, fica praticamente impossível descobrir a chave de decodificação, e tomar números cada vez maiores pode aumentar a segurança. Contudo, o método RSA possui limitações matemáticas e técnicas com relação à quantidade de dados que se pode armazenar. Além de que existem ataques capazes de descriprotografar as informações, como: o *método da força bruta*, que tenta descobrir todas as chaves privadas possíveis; o *timing attack*, que determina uma chave privada baseando-se no tempo que um computador leva para decifrar uma mensagem; e técnicas matemáticas para fatoração de N, para determinação de $\varphi(N)$ sem ter p e q, ou para determinar t sem ter $\varphi(N)$ (Cf. [2]).

Exemplo: Usando a criptografia RSA, vamos codificar a palavra AMIGO, e decodificá-la em seguida. O primeiro passo consiste em construir uma tabela que fará corresponder as letras do alfabeto a números. Escolhendo de maneira aleatória, vamos fazer a tabela da seguinte forma:

DOI: 10.5540/03.2015.003.01.0231

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

R	S	T	U	V	W	X	Y	Z	Á	É	Í	Ó	Ú	À	
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42

Obs.: Foi destinado um número para o espaço, e a numeração começou do 10 para evitar ambiguidades.

Devemos transformar a mensagem-texto em mensagem-numérica. Para isso, utilizaremos a tabela. Assim, a mensagem-texto 'AMIGO' corresponde à mensagem numérica '1022181624'. Para simplificar as contas, escolheremos números pequenos para p e q. Vamos fazer $p = 5$ e $q = 13$. Assim, $N = p.q = = 65$. Aplicando a função de Euler, temos que $\varphi(N) = \varphi(65) = 48$.

O próximo passo é escolher um número k para compor a chave de codificação. Devemos ter que $1 < k < \varphi(N)$ e $mdc(k, \varphi(N)) = 1$. Tomaremos $k = 11$. Assim, a chave pública (de codificação) é $(65, 11)$, e será usada da seguinte forma:

$$\text{(texto codificado)} \equiv \text{(texto original)}^{11} \ \ (mod\ 65)$$

Separaremos o texto-numérico em blocos de dois dígitos para codificar a mensagem. A maneira de separar a mensagem não é única, mas deve-se tomar cuidado, pois é necessário evitar que o bloco inicie com zero, e devemos ter cada número a_i do bloco $a_i < N$. Então: $b_i \equiv a_i^k \ \ (mod\ N)$, onde a_i é o texto original e b_i o texto codificado, com $i = 1, 2, ..., 5$. Daí, $b_1 \equiv 10^{11} \ \ (mod\ 65) \Rightarrow b_1 \equiv 30 \ \ (mod\ 65)$. Logo, 30 é a codificação de 10. De forma análoga, temos:
$b_2 \equiv 22^{11} \ \ (mod\ 65) \Rightarrow b_2 \equiv 03 \ \ (mod\ 65)$; $\ b_3 \equiv 18^{11} \ \ (mod\ 65) \Rightarrow b_3 \equiv 47 \ \ (mod\ 65)$;
$b_4 \equiv 16^{11} \ \ (mod\ 65) \Rightarrow b_4 \equiv 61 \ \ (mod\ 65)$; $\ b_5 \equiv 24^{11} \ \ (mod\ 65) \Rightarrow b_5 \equiv 24 \ \ (mod\ 65)$.
Portanto, a mensagem codificada é: 30 03 47 61 19.

Para encontrar a chave de decodificação, basta resolver a congruência $11t \equiv 1 \ \ (mod\ 65)$, que fornece $t = 35$. Logo, a chave privada (de codificação) é (65,35), e será usada da seguinte maneira:

$$\text{(texto original)} \equiv \text{(texto codificado)}^{35} \ \ (mod\ 65)$$

Para verificar que o método RSA funcionou, vamos decodificar a mensagem:
$a_1 \equiv 30^{35} \ \ (mod\ 65) \Rightarrow a_1 \equiv 10 \ \ (mod\ 65)$; $\ a_2 \equiv 03^{35} \ \ (mod\ 65) \Rightarrow a_2 \equiv 22 \ \ (mod\ 65)$;
$a_3 \equiv 47^{35} \ \ (mod\ 65) \Rightarrow a_3 \equiv 18 \ \ (mod\ 65)$; $\ a_4 \equiv 61^{35} \ \ (mod\ 65) \Rightarrow a_4 \equiv 16 \ \ (mod\ 65)$.
$a_5 \equiv 19^{35} \ \ (mod\ 65) \Rightarrow a_5 \equiv 24 \ \ (mod\ 65)$
Perceba que a mensagem-numérica que as contas retornaram (10 22 18 16 24) coincidem, de acordo com a tabela, com a mensagem-texto 'AMIGO', como queríamos.

A criptografia RSA não é a única, porém é uma das mais eficientes. Destacamos a RSA, mas nosso trabalho se estende a outras criptografias baseadas na Congruência Modular. Algumas ainda mais simples do que a RSA.

Palavras-chave: *Matemática Discreta, Congruência Modular, Criptografia, RSA*

Referências

[1] FREIRE, Benedito T. V. **Notas de Aula - Teoria dos Números**. Disponível em: <http://www.olimpiada.ccet.ufrn.br/wp-content/uploads/2013/08/NOTAS-DE-AULA_09.pdf> Acesso em: 06 dez. 2013.

[2] LÓPEZ, Javier G.; MEURER, Lúcio A. **Estudos dos Ataques Matemáticos ao RSA e Hipótese de Modificação do Algoritmo.** Disponível em: «http://sedici.unlp.edu.ar/bitstream/handle/10915/22344/Documento_completo.pdf?sequence=1» Acesso em: 09 abr. 2014.

[3] OLIVEIRA, Maykon C. de. **Aritmética: criptografia e outras aplicações de congruências**. 2013. 63p. Monografia (Mestrado). Universidade Federal de Mato Grosso do Sul, Campo Grande, 2013.

