Criptografia: Parte 08 (Método RSA-1)

Mário Leite

...

A criptografia de chave única (como nos casos de “Cifragem de Cesar” e “Cifra de Vigenère”) pode ser uma solução para os casos em que a mensagem não seja tão valiosa. Mas, como o termo “valiosa” é muito relativo, o ideal é dar à mensagem a melhor proteção possível, pois, é melhor acertar por excesso do que errar por omissão! E a forma mais eficiente de fazer isto é utilizar uma **Criptografia de Chave Dupla**, em que são utilizadas duas chaves para tratar a mensagem: uma só para encriptar e outra só para decriptar. A chave de encriptação é chamada “chave pública”; e como o termo sugere, pode ser do conhecimento de todos. Já a chave para decriptar, chamada de “chave privada”, é usada somente para decriptar a mensagem e deve ser preservada dos olhos alheios! Um destes métodos, utilizado pela maioria dos profissionais, é conhecido como **Sistema RSA** cuja sigla foi retirada da primeira letra dos sobrenomes de seus criadores: Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman. O algoritmo deste método pode ser resumido nos seguintes passos:

1) Selecionar a mensagem a ser criptografada (codificada).

2) Fazer uma pré-codificação da mensagem, caractere por caractere, baseada em uma tabela qualquer (evitar a tabela ASCII) como a **tabela RSAI.1** que faça a correspondência de um número com cada caractere da mensagem.

3) Escolher dois números primos (**p**,**q**) bem grandes e não sequenciais.

4) Criar um número **n=p*q**, com p e q sendo mantidos secretos, embora **n** possa ser tornado público.

5) Quebrar a mensagem em blocos numéricos de modo que cada bloco seja menor que **n**, e certificar que nenhum deles comece com **0** (zero).

6) Selecionar um número **e** que seja coprimo com a Função de Euler ϕ(n) para criar a chave pública (**e**,**n**) que irá codificar a mensagem.

Observe que o quarto passo do algoritmo diz que **n** pode ser publicado, mas, **p** e **q** têm que ser mantidos secretos (apenas quem codifica a mensagem pode conhecê-los); e para conhecê-los uma solução seria “fatorar n”; mas isto se tornaria inviável para números muito grandes, e mesmo que se consiga a fatoração usando um cluster de CPU´s, descobrir os dois números primos que deram origem à chave de encriptação seria um colossal esforço computacional. É aí que está a eficiência do método RSA pois, fatorar um número muito grande pode levar anos; e por incrível que pareça, uma mensagem encriptada com uma chave pública de 1024 *bits* (número de 309 dígitos) poderia levar até dezenas de milhares de anos para ser decriptada (decodificada), mesmo utilizando *cluster* de CPU´s de computadores de grande porte!

Como exercício desta teoria, vamos analisar o exemplo de *codificação/decodificação* da simples mensagem “**O BEBE BABA**”.

Continua com o “Método RSA-2” (Parte 09)

Caractere	Código	Caractere	Código
A	10	N	23
B	11	O	24
C	12	P	25
D	13	Q	26
E	14	R	27
F	15	S	28
G	16	T	29
H	17	U	30
I	18	V	31
J	19	W	32
K	20	X	33
L	21	Y	34
M	22	Z	35
		<espaço>	55

Tabela RSAI.1 - Definição dos caracteres da criptografia