

Criptografia: Parte 9 (Método RSA-2)

Mário Leite

...

Continuando com as etapas mencionadas na **Parte 8**...

1 - Etapa de Pré-codificação

1.1 - Selecionar a mensagem a ser codificada: "O BEBE BABA".

1.2 - Pré-codificar a mensagem de acordo com uma tabela; por exemplo, seja a que foi mostrada na **tabela RSA1.1** da **Parte 8**.

Note que naquela tabela foram consideradas apenas letras maiúsculas e mais o espaço cujo código foi convencionado como **55**. Então, a mensagem pré-codificada fica assim: **2455111411145511101110**

1.3 - Considerar dois números primos: **p** e **q**: exemplo, **17** e **23** (como exemplos didáticos).

1.4 - Fazer **n = p*q = 391**

1.5 - Separar a mensagem em blocos de tamanho menor que **n**, com os seguintes valores: **245 51 114 11 145 51 110 11 10** (separados em nove blocos).

E para uma maior segurança é importante que cada bloco não indique nenhuma unidade ou sequência linguística que possa ser conhecida num idioma; por exemplo, **65 66 67** (o que seria **ABC** no código ASCII); isto deve ser evitado. E os blocos não precisam ser, necessariamente, todos de um mesmo tamanho mas, não podem começar com **0** e nenhum deles pode exceder a **n**.

2 - Etapa de Codificação

Cada bloco **b** ($0 < b \leq n$) é codificado assim: **C(b) = b^e mod n**, onde "**e**" representa o elemento que compõe a chave pública (**e,n**). No caso foi considerado **e=3** como expoente de cada código de letra, uma vez que **3** é um dos **352** coprimos com **φ(n)=φ(391)**, sendo **φ** a função de Euler. A codificação é feita na função "CodifTexto()" do programa "ProgRSA" (que será visto mais tarde); e depois de ter sido conhecido o valor de "**e**" na função "ChavePub()" deve ser calculados os termos **B's** do bloco numérico.

B1	245:	(245 ³ mod 391)	=	(14706125 mod 391)	=	224
B2	51:	(51 ³ mod 391)	=	(132651 mod 391)	=	102
B3	114:	(114 ³ mod 391)	=	(1481544 mod 391)	=	45
B4	11:	(11 ³ mod 391)	=	(1331 mod 391)	=	158
B5	145:	(145 ³ mod 391)	=	(3048625 mod 391)	=	389
B6	51:	(51 ³ mod 391)	=	(132651 mod 391)	=	102
B7	110:	(110 ³ mod 391)	=	(1331000 mod 391)	=	36
B8	11:	(11 ³ mod 391)	=	(1331 mod 391)	=	158
B9	10:	(10 ³ mod 391)	=	(1000 mod 391)	=	218

Continua com o "Método RSA-3 (Parte 10)