

Criptografia: Parte 10 (Método RSA-3)

Mário Leite

...

Continuando com as etapas mencionadas na **Parte 9**...

3 - Etapa de Decodificação

Nesta etapa é calculado o parâmetro **d** da chave privada (**d,n**); e neste caso os cálculos matemáticos envolvem aritmética modular, conceitos de inversibilidade de módulos de números, etc. Aqui vamos considerar que para os valores de **p** e **q** o valor de **d** é 235, com **e=3**. A decodificação deve ser feita tomando o resto da divisão por **n** de **C** elevado a **d** para cada bloco encontrado anteriormente na etapa de codificação; assim teremos, finalmente, a decodificação de cada letra da mensagem codificada. Então, chamando de **C** cada código de letra da mensagem, é obtido o seguinte esquema:

C1 224: $(224^{235} \bmod 391) = (2.033687...^{552} \bmod 391) = 245$
C2 102: $(102^{235} \bmod 391) = (1.049639...^{472} \bmod 391) = 51$
C3 45: $(45^{235} \bmod 391) = (3.198458...^{388} \bmod 391) = 114$
C4 158: $(158^{235} \bmod 391) = (4.835211...^{516} \bmod 391) = 11$
C5 389: $(389^{235} \bmod 391) = (4.346666...^{608} \bmod 391) = 145$
C6 102: $(102^{235} \bmod 391) = (1.049639...^{472} \bmod 391) = 51$
C7 36: $(36^{235} \bmod 391) = (5.383784...^{365} \bmod 391) = 110$
C8 158: $(158^{235} \bmod 391) = (4.835211...^{516} \bmod 391) = 11$
C9 218: $(218^{235} \bmod 391) = (3.445688...^{549} \bmod 391) = 10$

A decodificação pode ser comprovada juntando os blocos para recriar a mensagem.

24 O
55
11 B
14 E
11 B
14 E
55
11 B
10 A
11 B
10 A

A pergunta é a seguinte: “Como são feitos os cálculos pesados de módulos mostrados no exemplo de codificação/decodificação da mensagem “O BEBE BABA”?! Por exemplo, como fazer o cálculo para decodificar a quinta letra (“E”) desta mensagem?!

C5 389: $(389^{235} \bmod 391) = (4.346666...^{608} \bmod 391) = 145$

Problema: Como fazer os cálculos “pesados” deste método!?

Continua com o “Método RSA-4 (Parte 11)