172 **O MÉTODO RSA DE CRIPTOGRAFIA.** *Leandro C. Merlo, Bárbara D. Amaral, Vilmar Trevisan* (Departamento de Matemática Pura e Aplicada - Instituto de Matemática – UFRGS)

No início dos anos 70, com o incremento do número de transações comerciais via canal aberto (comunicação de dados), tornou-se necessária a elaboração de sistemas de criptografia com chave pública. O desafio era obter um método cuja codificação fosse pública, mas a decodificação deveria ser difícil sem uma (outra) chave mantida em segredo. Neste trabalho descreveremos o método RSA, atualmente muito usado com o avanço da rede mundial de computadores, que satisfaz estes critérios e é baseado em teoria dos números. A codificação é feita via exponenciação da mensagem módulo n=p.q, com p e q números primos. A decodificação pode ser feita caso p e q sejam conhecidos, o que torna a quebra do sigilo difícil, uma vez que não existem métodos eficientes para a fatoração de números inteiros.