197 **NÚMEROS INTEIROS E CRIPTOGRAFIA RSA.** *Maira Maria Marin, Alveri Alves Sant Ana (orient.)* (UFRGS).

A Criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. Hoje em dia, a comunicação entre computadores via Internet vem criando novos desafios para a criptografia, uma vez que é necessário codificar as mensagens envidadas, sempre que contenham informações importantes, como em transações comerciais ou bancárias, por exemplo. O mais conhecido dos métodos de criptografia de chave pública é o RSA, que foi criado em 1978, pelos matemáticos Rivest, Shamir e Adleman. Para implementar o RSA precisamos de dois parâmetros que são dois primos muito grandes p e q. Para codificar uma mensagem precisamos conhecer o produto destes dois primos e para decodificar precisamos conhecer p e q. Portanto a chave de codificação do RSA é constituída essencialmente pelo número n = pq e esta chave é tornada pública. Já a chave de decodificação é mantida secreta por cada usuário. A segurança do método vem do fato de que utilizamos primos p e q muito grandes, fazendo com que as tentativas de interseptação de mensagens esbarrem em obstáculos de natureza tecnológica, pois se tivermos p e q muito grandes (150 algarismos ou mais) fatorar n para encontrar p e q , utilizando os métodos atuais, levaria alguns milhares de anos. Pretendemos, com este trabalho mostrar como e porque o método funciona, discutindo também a segurança do mesmo. (PIBIC).