045 **UM ESTUDO SOBRE O ATAQUE DE WIENER AO RSA.** *Israel de Souza Rocha, Vilmar Trevisan (orient.)* (UFRGS).

O sistema de criptografia de chave-pública RSA (Rivest-Shamir-Adleman) é bastante conhecido e largamente utilizado atualmente, visto que existem algoritmos eficientes para todas operações envolvidas, porém não se conhece nenhum algoritmo eficiente para reconstruir a mensagem cifrada sem o conhecimento da chave-privada. Entretanto, em certos casos, podemos encontrar a chave-privada usando frações contínuas. Mostraremos nesse trabalho o algoritmo de Wiener para ataque ao RSA. No algoritmo é encontrado o expoente privado d com complexidade $O(\log N)$, quando a chave-pública (N, e), onde $N=pq$, é tal que $q<p<2q$ e $d<1/3*N^{0,25}$. A chave-pública é utilizada para criar uma estimativa próxima do expoente privado, fazendo uso de sua expanção em frações contínuas. Inicialmente, algumas propriedades de frações contínuas finitas e infinitas foram pesquisadas. Após, o estudo se concentrou em utilizá-las como um método para obter aproximações de números reais. Em seguida, implementou-se o algoritmo proposto no trabalho de Wiener, realizando testes para alguns tamanhos de chave semelhantes aos utilizados hoje em dia. Em seu artigo, Wiener também sugere modificações no uso do RSA para evitar o ataque. Uma delas é fornecer infomações sobre p e q na chave-pública, ao invés apenas do produto pq. Dessa forma a chave-privada pode ser maior sem comprometer o tempo das operações que a utilizam. (Fapergs).