270 **MÉTODOS PARA O CÁLCULO DO LOGARITMO DISCRETO.** *Denise Temp Flores, Vilmar Trevisan* (Instituto de Matemática, UFRGS).

Criptografia é o estudo de métodos para enviar mensagens em forma codificada (disfarçada) de modo que somente o receptor possa remover o disfarce (decodificar) e ler a mensagem com o auxílio de uma chave. A segurança desses métodos é medida pela dificuldade que um espião tem para decifrar a mensagem sem o conhecimento da chave. Muitos criptosistmas são baseados no fato de que logaritmos discretos são difíceis de calcular. Se x e b são conhecidos, calcular $y=b^x$ é fácil em qualquer grupo. Se y e b são conhecidos, é fácil calcular x no caso de grupos contínuos. Já no caso de grupos discretos, a determinação de x, chamado logaritmo discreto, é um problema muito difícil, se o número de elementos do grupo é grande. Nosso objetivo neste trabalho é apresentar três métodos para o cálculo do logaritmo discreto em um corpo finito $Z/(p)$, que são conhecidos por método de Shanks, método de Silver-Pohlig-Hellman e ``index calculus''. (PROPESQ/UFRGS)