062 **FERRAMENTAS DE AUXÍLIO À CRIPTOANÁLISE DE CIFRAS DE SUBSTITUIÇÃO.** *Eduardo Bobsin Machado, Raul Fernando Weber* (Departamento de Informática Pura e Aplicada, Instituto de Informática, UFRGS)

Cada vez mais a criptografia e a segurança se tornam parte de nosso cotidiano. Pensando nisso, foram desenvolvidas duas ferramentas para a criptoanálise de cifras de substituição, que também auxiliam no estudo do assunto em uma disciplina de graduação. A primeira auxilia na decifragem de textos encriptados com cifras de deslocamento. O segundo programa é utilizado para encriptações de substituição com o uso de tabelas sobre o alfabeto (A-Z). Ambas foram desenvolvidas com o compilador Borland C++ Builder 3 e podem ser utilizadas tanto para cifragem quanto para decifragem de mensagens. O uso destas vem a comprovar que as técnicas de criptografia ditas manuais ou mecânicas estão obsoletas devido ao poder computacional disponível atualmente. Para manter um nível de segurança satisfatório, utiliza-se criptografia computacional nos dias de hoje. (CNPq/RHAE)