SCHOOL OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING
MONASH UNIVERSITY

TECHNICAL REPORT 2004/155

Pedagogically Sound Examples in Public-Key Cryptography

S K Chong, G E Farr, L Frost and S Hawley

ABSTRACT

Pencil-and-paper exercises in public-key cryptography are important in learning the subject. It is desirable that a student doing such an exercise does not get the right answer by a wrong method. We therefore seek exercises that are *sound* in the sense that a student who makes on of several common errors will get a wrong answer. Such exercises are difficult to construct by hand. This paper considers how to do so automatically, and describes software developed for this purpose, covering several popular cryptosystems (RSA, Diffe-Hellman, Massey-Omura, ElGamal, Knapsack). We also introduce *diagnostic* exercises, in which all error paths lead to different answers, so that the answer given by the student may suggest the nature of their error. These too can be generated automatically by our software.