USING THE TI-92 PLUS TO INTRODUCE THE RSA CRYPTOSYSTEM

Robert T. Harger and Neil P. Sigmon

1. Introduction. With society becoming more and more reliant on digital and computing technology, the ability to transfer information in a secure and confidential fashion using cryptography, the art of secret message writing, has increased dramatically in importance. As this reliance increases in the future, people will benefit in having at least some basic knowledge of this important topic. However, most students, especially those majoring in liberal arts and humanity curriculums, have no formal training in any of the mathematics techniques that are used in cryptography. Much of this problem stems from the fact that many cryptographic techniques are too tedious to perform by hand and rely on computing technology not readily available to all students for performing realistic examples.

To alleviate this problem, the topic of cryptography has been integrated into our finite mathematics course. This course, which exposes students to topics such as linear equation applications, matrices, and mathematics of finance, is designed to introduce some of the many "real-life" applications of mathematics. Preliminary evaluations from students have shown a favorable response for integrating cryptography into this course. As a part of this topic, the RSA Cryptosystem, currently one of the most widely used cryptosystems, is introduced. This cryptosystem is simplistic in its application in that one has to only understand the concepts of exponentiation and modular arithmetic to implement it. However, realistic applications of this system require large integers, which makes it impractical to compute by hand. Fortunately, the algorithms necessary to perform the computations required for the RSA Cryptosystem can easily be programmed into a TI-92 Plus graphics calculator.

The purpose of this article is to demonstrate how the RSA Cryptosystem is integrated into our finite mathematics course. In particular, we discuss how the TI-92 Plus plays an integral part in performing the needed computations. As a point of information, every student is required to have a TI-92 Plus (or TI-89) for our course. We first give a discussion of some basic background mathematics.

2. Preliminary Concepts. The RSA Cryptosystem relies on concepts from number theory that are familiar to most students; exponentiation, prime numbers, greatest common divisors, and modular arithmetic. All the numbers we work with in this paper are nonnegative integers. When denoting exponentiation we will use