

University of Western Australia
DEPARTMENT OF MATHEMATICS
**UWA ACADEMY
FOR YOUNG MATHEMATICIANS**

Introductory Comments

Greg Gamble

April 8, 1997

The next series of lectures will be on topics related to Number Theory (which deals with the mathematics of whole numbers). We explore divisibility, prime numbers and some applications. In this area of mathematics a calculator is often quite useless. (For example, try to find the last digit of:

$$7^{7^{7^{7^7}}}$$

using a calculator!) A more interesting problem is that of trying to send a message *secretly*. What one wants are two black boxes – one that encrypts a message for sending and another that the message recipient uses for decrypting it. There is a very nice (easy-to-apply) Number Theoretic way of doing this (the RSA system) based on having an integer n with two very large prime divisors. (We tend to use a computer to perform the black box algorithms, but the ideas are quite elementary.) Some students may have heard of PGP (Pretty Good Privacy), a program commonly used to encrypt/decrypt email messages. PGP uses the RSA system.