

ANU COLLEGE OF SCIENCE

DEPARTMENT OF MATHEMATICS

ONE-DAY PROFESSIONAL DEVELOPMENT COURSE

INTERNET SECURITY, NUMBER THEORY & RSA CRYPTOGRAPHY

For Mathematics and IT Teachers, ACT Secondary Colleges & High Schools

When: CHANGE OF DATE to Friday June 2, 9.30am – 4.00pm

Where: Arndt Lecture Theatre 1, Arndt Building, ANU campus end of Kingsley Street, off Barry Drive

Cost: Free. Morning tea, lunch and afternoon tea provided

Organised by the Department of Mathematics, ANU

RSA cryptography is the basis of all internet banking, and all Amazon and Ebay transactions. It has the amazing property that you (or your computer) can tell everyone in the world how to code a secret message to you. Anyone may publish their coded secret message to you for everyone else to see, but only you hold the keys to decipher the coded message. Not even the CIA, Mossad, or the KGB could crack your code in a thousand years.

The method, discovered in 1977 by 3 mathematicians, relies on the difficulty of factoring large numbers and on a little number theory.

In this course we will discuss the algorithm for RSA cryptography and the mathematics behind it. You can even implement it in our computer labs. Extensive notes will be provided.

ANU secondary college: RSA cryptography is a major topic in the first of the four half units in the new maths minor course for selected years 11 and 12 students. The text is *The Heart of Mathematics* by Burger and Starbird, supplemented by the notes *An Introduction to Contemporary Mathematics* (latest version at www.maths.anu.edu.au/~john/secondarycollege)

The teachers involved will discuss their experiences with the course. There will also be time for discussion of pedagogy.

We are planning 3 more courses: A Hierarchy of Infinities, 2006; Geometry & Topology, 2007; Chaos & Fractals, 2007.



Mona Lisa with Keys, Fernand Leger, 1930

MORE INFORMATION

Registration, Administrative Information, Parking Vouchers: Katie.Lau@maths.anu.edu.au
(Please register early; we would like an early estimate and may need to restrict numbers)

Course Information: John.Hutchinson@anu.edu.au