CRYPTOGRAPHY MTH6115
COURSE INFORMATION

LECTURER: Bill Jackson, Room 253, Mathematics Building

LECTURE TIMES: Tuesday 1-2 in CMLT, Tuesday 3-4 in Physics Lecture Theatre, and Thursday 9-10 in Geography 126.

EXERCISE CLASSES: Wednesday 11-12 in Arts G02 and Thursday 2-3 in CS338, starting in the second week of the semester.

OFFICE HOURS: Wednesday 1.30-2.30 and Thursday 3.30-4.30

RECOMMENDED BOOKS:

> Simon Singh, *The Code Book: The Secret History of Codes and Code-Breaking*, Fourth Estate, London, 1999 (introductory).
>
> Douglas Stinson, *Cryptography: Theory and Practice*, Chapman and Hall.
>
> Dominic Welsh, *Codes and Cryptography*, Oxford University Press.

COURSE NOTES: A set of notes written by Peter Cameron with minor revisions made by Rob Wilson when they gave the module can be found on the course web page:
http://www.maths.qmul.ac.uk/ bill/MTH6115/

WEEKLY EXERCISES: These will be handed out each week at the beginning of a Tuesday lecture, starting with the second week of lectures. Your solutions should be placed in the BLUE BOX on the SECOND FLOOR of the Mathematics Building no later than 4.30 p.m. on the Tuesday of the following week. I will put my solutions to the exercises on the course web page. Note that I and markers will be on the watch out for signs that students have been copying from each other. Any students found doing so will receive a zero mark for that exercise, whether they are the ones who did the copying or the ones who allowed their solutions to be copied. Collaboration between students in tackling these exercises is allowed, but any student allowing other students to copy their solutions will be doing them a disservice - they will learn nothing from it and consequently will probably fail the examination next May.

The total in-course contribution to the final mark for the course will be 30%, and the final examination will contribute 70%.