Queen Mary
University of London

MAS 335 Cryptography

Course Information Spring 2008

Lecturer: Professor R. A. Wilson **Email:** R.A.Wilson@qmul.ac.uk

Lectures:	Monday	09:00–10:00	Mathematics Lecture Theatre
	Monday	11:00–12:00	Mathematics Lecture Theatre
	Tuesday	13:00–14:00	Mathematics Lecture Theatre

There will be no lectures in Reading Week (week 7), when the Cipher Challenge (see below) will take place.

Exercise Classes:	Monday	14:00-15:00	CS 446	Surnames L–Z
	Tuesday	15:00-16:00	Engineering 324	Surnames A–K

[Exercise classes will be held as needed, starting in week 3. Please try to stick to your allocated slot, unless you have a clash with another course.]

Assessment: The course assessment is **30% coursework, 70% final exam**. The coursework component is divided equally between the **exercise sheets** and the **cipher challenge**.

There will be approximately six coursework sheets, for handing in in weeks 3, 4, 5, 9, 10, 11. (NB: these arrangements are provisional, and may change.) The best five marks out of six will count for 15% of the total marks. Coursework must be handed in not later than **Thursday at 3.30pm**, to the RED box on the SECOND floor, in the appropriate weeks.

Remember: The work you hand in should be your OWN work. If you work in groups make sure you YOURSELF understand the answers that have been obtained, and write up your answers YOURSELF. I take a dim view of copied answers, and will penalise them severely when I detect them.

There is also a “cipher challenge” where you encipher some text and the rest of the class has the opportunity to break your cipher; this will also count for 15% of the total marks. Arrangements for the cipher challenge will be announced later.

PTO

Course Web page: Course material (including problem sheets, lecture notes, announcements, and the cipher challenge) will be kept at

`http://www.maths.qmul.ac.uk/%7Eraw/MAS335/`

Please consult this page regularly for updates, especially if you are in the habit of missing lectures and therefore also missing announcements!

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.

CALCULATORS ARE NOT PERMITTED
in the examination for this course.

Robert A. Wilson
3 January 2008