Queen Mary
University of London

MAS 335 Cryptography

Assignment 3 **For handing in on 16 February 2005**

The Cipher Challenge

This homework consists of taking a piece of plaintext in English and enciphering it. All ciphers received will be placed on the Web, at
`http://www.maths.qmul.ac.uk/~raw/MAS335/ciphers/`
and you may then attempt to break other people's ciphers.

Here are the rules. Failure to obey these rules could result in loss of marks.

(a) The plaintext must consist of between 500 and 1000 characters. The ciphertext should not be longer than 1500 characters.

(b) You must not use a computer program for the encryption unless you write it yourself: if you do, you must include the program text in your submission.

(c) You must explain your method of encryption, including full details (so that I can decrypt it and check your work), in no more than 500 characters. (If you want to add a second and more complete explanation, you may; but the short explanation must contain full details.)

(d) You must email your plaintext, ciphertext, and explanation to me (`r.a.wilson@qmul.ac.uk`) as a *plain text file*. Other types of file (Word document, PDF, etc.) will result in loss of marks. Include your name and student number in the email.

(e) You will be awarded up to 20 marks for the cipher and up to 40 for the description of the encryption. If your cipher is broken, you lose 10 marks. The first person to break the cipher gets up to 40 marks (10 for the correct plaintext, 30 for a description of the method); the second and third person to break the cipher get up to 20 and 10 marks respectively. You may attempt to break as many ciphers as you wish, but nobody is eligible for more than 40 marks for this part of the challenge.

(f) The deadline for the receipt of entries is **Wednesday, 16 February 2005**, and the deadline for breaks of other people's ciphers is **Thursday, 24 March 2005**.