Queen Mary
University of London

MTH6115 Cryptography

Cipher Challenge: Part 1 For handing in on 7th February 2011

This assignment is for e-mailing directly to me in the format specified below.

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/%7Ejnb/MTH6115/CipChall11.html`
and you may then attempt to break other people's ciphers. Detailed instructions for this stage will be placed on this webpage.

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

(a) The plaintext must consist of between 700 and 1400 characters, excluding spaces and punctuation. It should be written in ordinary English (no foreign languages, excessive numbers of names, excessively technical terms, etc.), with no numerals. The ciphertext should not be longer than 2000 alphanumeric characters. Please use only UPPER CASE letters and numbers (and spaces) in the ciphertext. The hyphen and full stop can be used to separate out the individual "characters" of the ciphertext, if this is necessary for disambiguation.

(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 should limit your ciphers to the ciphers and ideas contained in the first 8 lectures, first 3 sets of course notes [up to the end of the stuff about Vigenère ciphers] or on the first 2 exercise sheets. (So no Enigma or autokey ciphers: sorry!) If you have any doubts about whether your cipher meets the requirement, ask me [well] before the deadline.

(d) You must explain your method of encryption, including full details (so that we 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, including ALL KEYS.

(e) Also include (not in the above 500 character limit) an explanation of how Bob (not Eve) should decrypt the cipher.

(f) You must e-mail your plaintext (and message), ciphertext, and explanations (including how Bob should decrypt the message) as a *plain text file*, with at most 80 characters per line. Other types of file (Word document, PDF, etc.) will result in loss of marks. Include your full name and student number in the e-mail. Your ciphers should be e-mailed to me at `J.N.Bray@qmul.ac.uk`. *It is your responsibility to ensure that your mailer does not truncate the ends of lines of your ciphertext.*

(g) This coursework counts for 5% of the total mark for this module. You will be awarded a mark out of 100: up to 30 marks for the cipher, up to 45 for the description of the encryption, and up to 25 for your description of how Bob should decrypt the cipher. If your cipher is broken, you will lose 25 marks. I reserve the right to modify this depending on how difficult I perceive your cipher to be.

(h) The deadline for the receipt of entries is **3:30 pm, Monday, 7th February 2011** and I shall aim to have the ciphers on the webpage by **2:00 pm, Friday, 18th February 2011** (subject to change) so that you can begin trying to break other people's ciphers.