

# IY2760/CS3760: Coursework 1

Coursework must be submitted electronically, as an email attachment, to the following email address: [c.mitchell@rhul.ac.uk](mailto:c.mitchell@rhul.ac.uk).

Coursework submissions should normally be in the form of a single pdf file.

Take care to ensure that you include your full name on the first page of your submission, and also the coursework number.

1. Compile a glossary of 25 commonly used security terms. A good starting point is the glossary of IT security terminology at the ISO/IEC JTC1 SC27 web site – see:

<http://www.jtc1sc27.din.de/en>

2. What is the main purpose of an encryption algorithm?
3. What is an exhaustive key search? What property is required of an encryption function to ensure that such a search is infeasible?
4. Find two four-letter words that yield the same ciphertext using the Caesar cipher (under two different keys). E.g. *bee* and *loo* both encipher to *mpp* – in the first case using a key which shifts every letter forward through the alphabet by 11 places, and in the second case using a key which shifts every letter by one place).
5. Describe how a simple substitution cipher works. How would you set about writing a computer program to automatically cryptanalyse ciphertext produced using a simple substitution cipher? You need only provide a *top level description* of the program.
6. Explain in your own words the properties needed for a stream cipher key stream to be secure. How do these properties relate to the key stream used in a one-time pad?
7. The Vigenère cipher can be considered as a type of stream cipher. State what the keystream generator is in this case, and describe whether or not it meets the properties given in your answer to the previous question.
8. Discuss the security of triple DES (as opposed to DES) with reference to key length / key space and implementation issues.
9. What is a dictionary attack on a block cipher, and how can we ensure that such an attack is infeasible?

**DEADLINE: 23:59, Friday 14th October 2010**