

# Assignment 2

## Public key Infrastructure

Value: 20%

**Working:** Does the code actually work? (proved by sample runs and code inspection)

Particular points that I will be looking for:

- Login mechanism and password checking
- The user interface for the chat system
- Identification and selection of user to chat with
- Authentication between users wishing to communicate
- Transmission of messages (including arbitrarily long messages) protected by session key
- Secure storage and retrieval of keys within the system
- The Certificate Authority (CA)
- The management interface and facilities for the PKI system
- How users are guaranteed that what they think is the CA's public key really is
- Certificate Structure
- Protection of CA private key
- Transmission of the private key to a user (for new user or replacement key)
- CRLs and their use
- Verification of Certificates
- Storage and retrieval of Certificates
- Generation of a Session key for use of users wishing to communicate

### Documentation

Comments (2 marks)

Sufficient so that a reader can understand your code (and whatever you think about your programming skills **no** program is entirely self documenting).

Compilation Instructions (1 marks)

Sufficient so that I could take your code and get it compiled

Purpose and user instructions (1 marks)

Sufficient so that someone who knows about encryption could work what your code is doing and how to use it. Also should include your name, student number and when you wrote the code – your should also include this information and a brief statement of what the code does as a header comment

Report (2 marks)

Properly formatted and clearly laid out.

# Assignment 2

## Security Policies

Value: 20%

I expect the report to be in decent written English. Marks may be deducted for poor spelling and/or grammar.

### **High Level Policies (6 marks)**

A good, representative selection of high level policies. Marks will be awarded for (among other things)

- Good choice of policies present, which represent a diverse selection of the necessary policies
- most sections of the organisation being covered within the selection (ie do not restrict yourself to policies for just one division)
- areas nominated in the assignment specification are covered
- Quality policies

### **Low Level Policies (6 marks)**

A good, representative selection of low level policies. Marks will be awarded for (among other things)

- Good choice of policies present, which represent a diverse selection of the necessary policies
- most sections of the organisation being covered within the selection (ie do not restrict yourself to policies for just one division)
- areas nominated in the assignment specification are covered
- Quality policies

### **Implementation Plan (4 marks)**

This should include:

- How is your security policy to be implemented?
- What steps are to be taken to ensure the support and proper education of staff and management?

### **Grammar, Spelling, Layout and presentation (4 marks)**

The document should be well laid out and presented. It should contain no grammar and spelling mistakes. You should be aiming for a professional level of presentation (but note that does not mean overblown use of colours and graphics)