EXAMINATION PAPER PROFORMA

This form should be attached to every examination paper submitted to the Examinations Officer

Name of Unit / Element: **COMPUTER SECURITY**

Code Number: **IS53012A**

Number of Pages: 6

May the paper be backed? Yes / No
(Delete as appropriate)

May the paper be reduced? Yes / No
(Delete as appropriate)

Length of paper: **2 hours 15 minutes**

Number of students expected to sit paper: **40**

Are the students permitted to retain the paper? **No**

Name of member of staff responsible for paper (lead examiner): **Ida Pu**

Any other special requirements (graph paper etc): .....

.....

.....

I confirm that the above paper and the rubric (containing the required wording as agreed by College Board) has been correctly scrutinised and agreed by the Visiting Examiner. Also that, if applicable, the necessary copyright permission has been granted.

Signed: ..... Date: 6.4.2011

Name: .... CRESSEL ..... Department: **Computing**
(Block capitals)

UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

B. Sc. Examination 2011

Computing

IS53012A Computer Security

Duration: 2 hours and 15 minutes

Date and time:

There are five questions in this paper. You should answer no more than three questions. Full marks will be awarded for complete answers to a total of three questions. Each question carries 25 marks. The marks for each part of a question are indicated at the end of the part in [.] brackets.

There are 75 marks available on this paper.

Electronic calculators must not be programmed prior to the examination. Calculators which display graphics, text or algebraic equations are not allowed.

THIS PAPER MUST NOT BE REMOVED FROM THE EXAMINATION ROOM

Question 1

(a) Explain the meaning of the terms (i) *availability*, (ii) *authentication* and (iii) *accountability* (one sentence for each term). Consider a university policy according to which no examination grades can be released to students over a telephone. Describe a difficult situation that may be prevented by the policy in terms of the availability, authentication and accountability. [6]

(b) Explain what is the *absolute rate of English language* R in the context of information theory. Assume use of the lowercase letters only. Show all your calculation. [3]

(c) Consider a multi-user distributed system that provides subjects access to objects to perform operations. [8]

i. Explain what is meant by a *subject*, *object* or an *operation*. Provide an example for each of these.

ii. Explain the term *ownership policy*.

(d) Explain what *auditing* is in the context of software security. Consider the table below. What does the table try to summarise? Interpret and explain the contents presented in the table. [8]

	in-house	third party	independent
prerelease software	√		
postrelease software	√		
product range comparison		√	
preliminary evaluation		√	
evaluation		√	
research			√

Question 2

(a) Explain what is meant by *symmetric* encryption. List four purposes for which symmetric encryption is especially appropriate. [6]

(b) Demonstrate how Vernam cipher works using an example of plaintext "lotsofwork". [6]

(c) Decrypt the cyphertext "rjjyytsnlmyfyufwp" using the *shift-cipher*. The key is believed to be a $shift \in [3, 7]$ and the plaintext consists of English words. What is the precise value of the key? Show all your work. [8]

(d) Explain what a *security plan* is. List three factors that should be considered when developing a security plan. [5]

Question 3

(a) Distinguish terms *fault* and *failure* in the context of Software Security. Give an example for each concept described. Explain why a fault may or may not become a failure. [6]

(b) What are the main characteristics of a trusted operating system? Explain the differences between being a secure system and a trusted system. [9]

(c) Explain, with the aid of an example, what is meant by *physical separation* for security in a computing environment. [4]

(d) Describe briefly each of the access control mechanisms below in terms of ease of determining authorised access during execution, adding access for a new subject, deleting access by a subject, or creating a new object to which all subjects have access by default. [6]

i. per-subject access control list: one list for each subject tells all the objects to which that subject has access.
ii. access control matrix.

Question 4

(a) Consider an environment where several users share access to a single database. Explain, with the aid of an example, how *indefinite postponement* can occur. What is the alternative term for an indefinite postponement? [6]

(b) Consider the segment of a distributed algorithm below for requests to a remote central classroom-booking system from two separate departments at different locations.

```
Department of Music: SELECT (CLASSROOM.NO='137A')
        ASSIGN 'D.Davis' TO  LECTURER.NAME

Department of Drama: SELECT (CLASSROOM_NO='137A')
        ASSIGN 'J.Jonason' TO LECTURER_NAME
```

Identify and describe a security flaw that the algorithm may cause. Modify the segment of the algorithm to solve the security problem. [7]

(c) Explain the difficulties in applying encryption on each field of database records. Assume the same key is applied to each data field of the entire database. [6]

(d) Explain what is meant by an *aggregate* measure, and what is meant by a *constituent* measure. Cite a situation in which the sensitivity of an aggregate is greater than that of its constituent values. [6]

Question 5

(a) Explain the term *end-to-end encryption.* Where and how can it be applied? [3]

(b) Explain what is meant by a *single point of failure* in the context of network security. Consider designing and running a web site for companies. Explain what issues can be seen as a single point of failure. [6]

(c) What techniques are often involved in a social engineering attack? What do the attackers aim to do? Describe a social engineering attack that can be used to obtain a user's password. [5]

(d) What is a stateless firewall? [5]

(e) Can encrypted email provide verification to a sender that a recipient has read an email message? Why or why not? [6]