UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

B. Sc. Examination 2012

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 what is meant by *linear vulnerability.*

Let $q_1, \cdots, q_5$ be 5 queries that do not reveal any single value of sensitive data $c_1, \cdots, c_5$ from a database. Demonstrate what relationships, if found, can be used to successfully devise the values of $c_1, \cdots, c_5$. [5]

(b) Demonstrate how the Vernam cipher works for the example of plaintext "computer" and the one-time pad (5 20 0 9 17 16 22 18). Explain why the cipher is hopeless in practice. [8]

(c) A salami attack is an attack in which the criminal can take a small amount from many bank accounts without being noticed, accumulating a valuable result. Describe briefly three controls that could be applied to prevent salami attacks. [6]

(d) Give a brief step-by-step account of *distributed denial of service* attacks. Comment on the seriousness of these attacks using some statistics. [6]

Question 2

(a) Describe Fermat's Little Theorem and demonstrate how the theorem can be used to check whether or not a given number n is a prime. Use $n = 7$ and $n = 8$ as examples and show all your work. [5]

(b) The RSA public key cryptosystem was first published in 1977 and has managed to withstand 'years of intensive cryptanalysis'. Name and describe the one-way function at the heart of RSA that makes it possible. Demonstrate, with a small example, the characteristics of the *one-way function*. [5]

(c) Consider the following protocol (in the box) for Alice to sell her laptop to Bob:

> i. Alice gives the laptop to Bob.
> ii. Bob gives a cheque for the agreed purchase price to Alice.
> iii. Alice deposits the cheque.

Assume that Alice and Bob do not trust each other but the laptop is genuine. Answer the following questions:

i. Identify and describe a transition flaw in the protocol that is in favour of Bob. [3]
ii. Modify and re-write the protocol to prevent potential attack from Bob. [4]
iii. Explain why your protocol works better than the previous one, and under what assumption(s) it works. [3]

(d) Explain what is meant by a *stream cipher* and what is meant by a *block cipher*. Give one example of each type of cipher. [5]

Question 3

(a) One way of limiting the effect of an untrusted program is confinement: controlling what processes have access to the untrusted program, and what access the untrusted program has to other processes and data. Explain how confinement would be applied to the program *untrusted P()* below. Devise and outline the algorithm of its confining program `trusted P()`. [9]

untrusted P()

```
$sum \leftarrow 0$
for $i = 1$ to 10 do
    $sum \leftarrow sum + i$
end for
```

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

(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

Consider two scenarios: (i) Council CUNC and (ii) University UNIV as follows:

i. The *council CUNC* consists of 100 departments requiring a new trusted database system for personnel management. Each department consists of 5 to 25 full-time permanent members of staff and every employee has a dedicated, distinguished and permanent role to play, and no plan to change for the next 5 years. Each department already has its own database system that is run independently by its own system administrator.

ii. The small *university UNIV* has only 5 departments and offers both full and part time modes of employment. The permanent staff members of each department often do job sharing, and temporary staff members are hired from time to time. Each department consists of 30 equivalent full-time posts. The students, however, can only be registered as full-time students. The university requires a new central database system to provide services to all the departments, including a web-based university virtual learning environment, as well as a secure database system for internal personnel and financial data. The university is also under reformation in general due to its challenging future environment.

Answer the following questions and justify any choices and/or decisions made:

(a) Write concisely your view (in a few sentences) of each of the following comments.

[Hints: Indicate whether you agree or disagree first, then give your own view before any justification. Add assumptions or definitions if necessary.] [6]

i. The fact that there are far fewer departments in UNIV than in CUNC makes the design of a trusted database easier for UNIV than that for CUNC in terms of access control.

ii. It is no more complicated to design a database system for CUNC than for UNIV as the same security issues have to be investigated and addressed.

(b) Explain and demonstrate how a vulnerability analysis may be conducted for UNIV to devise the sets of (i) assets, (ii) users, (iii) operations. [6]

(c) Demonstrate how a lattice may be applied to devise a rigorous access control plan. How many security levels are necessary? [5]

(d) Design a proper schema for each of CUNC and UNIV. Highlight the sensitive attributes by drawing a box (or a circle) around its name. For example, if STAFF-NAME is a sensitive attribute with two non-sensitive attributes XXX and YYY, the 3-field schema would be represented as: [8]

$\boxed{\text{STAFF-NAME}}$	XXX	YYY

Question 5

(a) An electronic mail system has been equipped with an encryption/decryption mechanism for coding the main text of the email. Explain how such an electronic mail system could still be used to leak information and give one example of the attributes that can cause the leakage. [6]

(b) Alice has recently stopped replying to Bob's emails and Bob wants to know whether Alice reads the emails. Having failed to get any automatic system responses from Alice's email system, Bob comes up with a simple plan, that he will encrypt his emails to Alice and send only the encrypted emails to Alice.

i. Devise a problem description, as formal and concise as possible, for cases like this, where Bob's plan would serve as a solution to the problem. [3]

ii. Discuss whether or not Bob's plan would work. Explain why it would (or would not) work. [6]

(c) Explain the main differences between the approaches used in a *direct attack* and in an *indirect attack* in the context of Database Security. [3]

(d) Describe a situation in the airplane seat-booking system where the *two-phase update* function would be necessary. Explain why the function is necessary and outline the segments of possible programming statements in pseudo-code. [7]