UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

B. Sc. Examination 2014

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, from the point of view of a cryptanalyst, the use of *entropy* of a piece of message in the context of Computer Security. Give an example to demonstrate how the entropy can be calculated. [5]

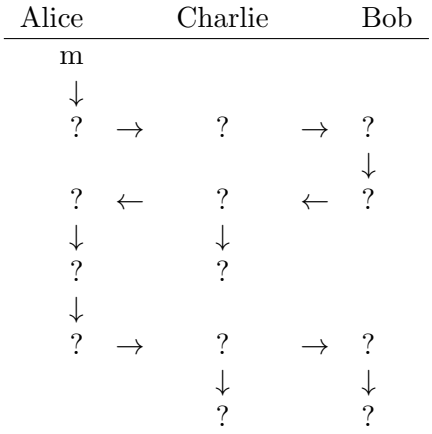
(b) The X Department of a university has two sections: *student* and *staff*. An employee can work for up to both sections. Information is classified as *open* or *private*. A security level is represented by a pair (x, y) where x is either open or private and y is a subset of the set (student, staff). A security level (x_1, y_1) dominates the security level (x_2, y_2) if $x_1 = x_2$ or if x_1 is private and x_2 is open, and if y_2 is a subset of y_1. [9]

i. How many security levels are there?
ii. Represent the access control structure by a lattice.
iii. Determine which security level dominates both the security levels (open, (student)) and the security level (private, (staff))

(c) What is the so-called *one-time key pad*? What is its main disadvantage? [5]

(d) To address the disadvantage of the one-time key pad, Frank proposes a cryptosystem that requires no key distribution and it works as follows:
`If she wants to send Bob a message` m`, Alice generates her key` a`, a sequence of random bits (the same length as` m`), computes` $c = m \oplus a$ `and sends` c `to Bob, where` $\oplus$ `represents the bitwise XOR operation. On receipt of` c`, Bob generates his own random bits` b `of same length, computes` $d = c \oplus b$ `and sends` d `to Alice. On receipt of` d`, Alice computes` $e = d \oplus a$ `and sends` e `to Bob. On receipt of` e`, Bob computes` $e \oplus b$ `for the last time.`

Annotate a diagram with logic expressions representing the message flow(s) using the format below, and explain why or why not Frank's cryptosystem works. [6]



Question 2

(a) A hash function can be used to produce a fingerprint of a file, a message, or other block of data. To be useful for message authentication, a hash function H must have the property that "H can be applied to a block of data of any size". Explain what would happen if H does not have this property. [5]

(b) List the names of two general options for ownership and five examples of possible permissions for a security policy. [2]

(c) Derive the access control table for a system with the following requirements: [5]

i. User Alex has read and write access to `game.exe` and has read, write and execute access to `letter.doc`.
ii. User Bill has read access to `game.exe` and `green.jpg`.
iii. User Carol has execute and read access to `letter.doc` and read access to `exam.java`.
iv. User David has the access to all the files.

(d) Consider a shift cipher, e.g., Caesar's cipher. Why is it easy to be broken? Demonstrate how difficult or easy to break the ciphertext "wklv phvvdjh lv qrw wrr kdug wr euhdn". Hence suggest a more appropriate way of using the cipher. Show all your work and represent the plaintext in capital letters. [13]

Question 3

(a) Explain, with the aid of an example, the vulnerabilities in the design and in the operation in terms of the software security. [6]

(b) Consider the two program segments *Program A()* and *Program B()* below. Comment on their functionality differences in the context of software security. What is a program like *Program B()*
often referred to as? What does *Program B()* essentially do to serve its purpose? [9]

Program A()

```
1: sum ← 0
2: for i = 1 to 10 do
3:     sum ← sum + i
4: end for
```

Program B()

```
1: x ← call Program A()
2: if x == expected (or use other reasoning to verify the result) then
3:     return 'success'
4: else
5:     return 'fail'
6: end if
```

(c) Describe the inference problem in the context of database security. Give an example of a direct attack on the sample databases below, highlighting the sensitive data fields. Add brief explanations or assumptions on data if necessary. [10]

Name	Sex	Race	Loans	Fines	Drugs	Address

Question 4

(a) Discuss *two* threats to password systems and describe *three* techniques that an intruder may use to gain unauthorised access to the systems. [9]

(b) Explain why encryption is rarely applied to implement separated fields in a database. Discuss two situations where (i) one key is applied to the entire database, and (ii) a different key is applied to each field of the database. [5]

(c) Describe what kinds of unauthorised disclosure can take place on the database. [6]

(d) Consider below an example of the statistics in a public report on the totals of the student financial aids by gender and department. Describe the characteristics of a potential *attack by sum* with the aid of the example. Specify one conclusion that can be drawn from the innocent data. Justify your answer and add assumptions if necessary. [5]

	Psychology £	Computing £	English £	Total £
Male	5000	3000	4000	12000
Female	8000	0	4000	12000
Total £	13000	3000	8000	24000

Question 5

(a) Consider each of the scenarios below and write down your advices, as a security expert to the general public, on what to do in each of the situations. Justify your answers, and, if necessary, add assumptions to ease your discussion.

i. You received a telephone call from your bank asking you to identify yourself before offering you a large overdraft. Assume that you would be interested in such a large overdraft but did not want to visit the bank. [4]

ii. You received an urgent request from your line-manager who lost his login password at an important overseas conference and asked you for the password. [4]

iii. You have to send one password to a remote site. [3]

(b) Discuss the challenges in continuous protocol development. Describe the "resurrecting duckling" protocol as an example of a protocol development that addresses an interesting security need before the need actually arises. [8]

(c) Consider design of a password system for a commercial bank. Explain briefly the terms (i) *integrity*, (ii) *non-repudiation* and (iii) *access control*. Give an example for each term. [6]