UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

B. Sc. Examination 2010

Computing

IS53012A(CIS326) 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 Fundamentals

(a) Demonstrate step by step an efficient way to compute $(3547 \times 2349) \bmod 11$. [5]

(b) Demonstrate how the Euclidean algorithm works for deriving the greatest common divisors $gcd(134, 28)$, and $gcd(3615807, 2763323)$. Show all your work. [5]

(c) Demonstrate how to compute 2^{15} with the minimum number of multiplications. Show all your work. [5]

(d) Explain what is meant by the term *collision* in the context of hashing, with the aid of an example (29, 93, 31, 159, 51, 189, 27, 23, 17, 9) and $h(k) = k \bmod 11$. [5]

(e) Consider the essential properties of a cryptographically strong hash function $y = H(x)$. One of the properties is that the hash function must be a one-way function. Describe two other essential properties, and explain why they are required. [5]

Question 2 Encryption and Cryptosystem

(a) Distinguish the concept of *computational security* from *unconditional security* of a cryptosystem. Explain why the unconditional security cannot be studied from the view point of computational complexity. [5]

(b) Describe Fermat's Little Theorem and demonstrate how the theorem can be used to determine $4^{11} \bmod 11$. What is the value of $3^7 \bmod 8$? Show all your work. [5]

(c) Describe a symmetric key exchange protocol which is based on the difficulty of solving the *discrete logarithm* problem. Explain how the protocol works for exchange of information between Alice and Bob. [10]

(d) Describe how the *rail fence cipher* works. Use the plaintext 'meet in park nine tonight' as an example. [5]

Question 3 Software Security

(a) Explain, with the aid of an example, what is meant by the *low level vulnerability* in the context of software security. [5]

(b) List five methods that an attacker can use to generate password guesses. Sort your list in order of the increasing degree of difficulty in terms of the number of estimated guesses. [5]

(c) Explain what a *Salami* attack is in the context of software security. Describe a classic example of the Salami attack that involves bank interest. Explain why it is difficult to detect the Salami attack. [5]

(d) Examine the following two claims about viruses. Write briefly about your view on the truth of each claim. [5]

i. It is better to use Linux, Unix or Macintosh than Windows systems because viruses can infect only Microsoft Windows systems.
ii. Viruses cannot remain in the main memory (RAM) after a complete power-off or power-on reboot.

(e) Consider the following program that computes the sum of the integers from 1 to 10.

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

An expert in software reusability and maintainability changes it to

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

Discuss a possibility that the second program can be sabotaged so that during the execution it computes a different sum such as 3 to 20. [5]

Question 4 Database Security

(a) 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

(b) Describe three main characteristics of multi-level database security. Use the table below as an example to support your description or arguments. Discuss and highlight two differences that may occur between the attribute-level sensitivity and data sensitivity. Add your own data if necessary for ease of discussion. [10]

Name	Department	Salary	Emails	Performance
Linda	Computing	40K	l.m@gold.ac.uk	A2
⋮	⋮	⋮	⋮	⋮

(c) Explain what is meant by *partitioning* in the context of multilevel security of databases. Discuss the disadvantages of partitioning. [5]

(d) Explain, with the aid of an example, what a *synchronisation flaw* is. [5]

Question 5 Network Security

(a) Examine the statements below regarding what firewalls can or cannot do. For each statement, mark a *true* or *false* and justify your answer. Rewrite each of the false claims to transform it to a true statement. [10]

i. Firewalls can protect an environment only if the firewalls control the entire perimeter.
ii. Firewalls can protect data near the perimeter.
iii. Data that have properly passed through the firewalls are safe.
iv. Firewalls are the most visible part of an installation to the outside so they are more attractive targets for attacks.
v. Firewalls must be correctly configured, updated, reviewed periodically.
vi. Firewalls are impenetrable. The smaller, the better.
vii. Firewalls exercise only minor control over the content admitted to the insider.

(b) Packet filtering gateways or screening routers are the simplest type of firewall. Describe the two other types of firewall named below. Explain how they work and what threats they intend to counter. [10]

i. Stateful inspection firewalls
ii. Guards

(c) Explain why PGP allows a user to have more than one key pair. [5]