UNIVERSITY OF LONDON

Goldsmiths College

B. Sc. Examination 2008

COMPUTER INFORMATION SYSTEMS

IS53012A(CIS326) Computer Security

Duration: 2 hours and 15 minutes

Date and time: May 2008

Answer THREE questions ONLY.
Full marks will be awarded for complete answers to THREE questions.
There are 75 marks available on this paper.
Electronic calculators may be used. The make and model should be specified on the script. The calculator must not be programmed prior to the examination. Calculators which display graphics, test or algebraic equations are not allowed.

THIS EXAMINATION PAPER MUST NOT BE REMOVED FROM THE EXAMINATION ROOM

Question 1

(a) Explain, with an example, what it is meant by *confidentiality* in the context of Computer Security. [5]

(b) A university department 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. [10]

(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) 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]

(d) Discuss the challenges in continuous protocol development. Describe an example of a new protocol that addresses interesting security needs. [5]

Question 2

(a) Explain, with an example, what is meant by *computer security.* [5]

(b) Describe the *discrete logarithm problem* for modular arithmetic. [5]

(c) Explain why compression, if any, should be done before encryption for a piece of message. [5]

(d) Discuss *two* threats to password systems and describe *three* techniques that an intruder may use to gain unauthorised access to the systems. [5]

(e) Consider passwords that consist of three uppercase alphabetic characters. Assume that it requires 5 seconds to test an individual password. Compute the time it would take to find a particular password in the worst case. Show all your working steps. If the passwords consist of up to three uppercase alphabetic characters, how does your answer differ? [5]

Question 3

(a) Consider a multi-user distributed system that provides subject accesses to objects to perform certain operations. Explain, with an example, what is meant by a *subject* and what is meant by an *operation*. [5]

(b) Consider the task of inserting data in the given order (3, 4, 5, 26, 6, 7, 23, 16, 39, 17, 22, 55) into a hash table H[0..22]. Suppose that the hash function $h(k) = k \bmod 23$ is used. Demonstrate the content of the hash table after the insertion using a linked list for closed addressing. Discuss the need for rehashing in this case. How many times would you attempt (the probing) before being successful? [10]

(c) Describe two different types of ownership. Give examples of *five* possible permissions to a file for a security policy. [5]

(d) Explain what an audit can offer in the context of software security. [5]

Question 4

(a) Suppose in a particular implementation it takes $20\mu s$ to do a modular multiplication when $b = 100$. Approximately how long would it take to do a modular multiplication when $b = 200$? [5]

(b) Encrypt the plain text "`VERNAMCIPHER`" using the Vernam cipher. Assume that the letters are represented with numbers 0 through 25 and the one-time pad is (76, 48, 16, 82, 44, 03, 58, 11, 60, 05, 48, 88). [10]

(c) Consider the access requirements below of a file system. Derive an access control table for the system in the following format. [5]

	rock.wav	game.exe	bebe.fig	file.doc
John	{}	{}	{}	{}
Sarah	{}	{}	{}	{}
Emma	{}	{}	{}	{}
Steve	{}	{}	{}	{}

(i) John has read and write access to 'rock.wav' and has read, write and execute access to 'game.exe'.

(ii) Sarah has read access to 'rock.wav' and 'bebe.fig'.

(iii) Emma has execute and read access to game.exe and read access to 'file.doc'.

(iv) Steve has all the access to any file.

(d) Explain what is meant by *high level vulnerability* in the context of software security. Give one example of such a vulnerability. [5]

Question 5

(a) Explain the two properties required for a *one-way function* in cryptography. Give an example of a one-way function. [5]

(b) Describe, with an example, Shannon's characteristics of Good ciphers. [5]

(c) An international commercial software company is proposed to set up a top-quality "tiger" team to conduct a series of security tests for a new software system. The main approach includes attempting the system to fail the tests. The testing will be considered as a "proof" of security: if it withstands the attacks, the system will be considered as secure.

Comment on the usefulness of the proposal and give your reasons. [15]