UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

Department of Computing

B. Sc. Examination 2016

IS53012A
Computer Security

Duration: 2 hours 15 minutes

Date and time:

This paper is in two parts: part A and part B. You should answer ALL questions from part A and TWO questions from part B. Part A carries 40 marks, and each question from part B carries 30 marks. The marks for each part of a question are indicated at the end of the part in [.] *brackets.*

There are 100 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

Part A

Question 1

(a) Write the missing words onto your answer book to form a truth statement: [4]

The hacker Charlie would use _____(1)_____ technique only as a last resort i.e. after he had tried _____(2)_____ and _____(3)_____ searching or if _____(4)_____ is very small.

(b) Write the missing words onto your answer book to form a truth statement: [2]

Compression, if any, should be done _____(1)_____ encryption for a piece of plaintext to strengthen cryptographic security because _____(2)_____.

(c) Write the missing words onto your answer book to form a truth statement:

A block cipher should have a large _____(1)_____ and _____(2)_____. [2]

(d) What other three properties should a well designed block cipher have? Explain what is meant by each of these properties and why they are essential for a block cipher. [6]

(e) Answer the following questions on Key Distribution. [6]

i. What is the benefit of adding authentication in Diffie-Hellman Key exchange protocol?
ii. Explain the difference between a session key and a master key.
iii. Briefly explain the anarchy model for distribution of public keys.

Question 2

(a) Consider a multi-user distributed system that provides subjects with access to objects to perform operations. Explain what are meant by a *subject*, *object* and an *operation*. Provide an example for each of these. [6]

(b) Answer the following questions on hash functions: [8]

i. Contrast MD-5 and SHA-1 in terms of efficiency, security and complexity.
ii. Can a Message Authentication Code (MAC) provide non-repudiation? Justify your answer.
iii. Can a MAC provide authentication? Justify your answer.
iv. Can hash functions be used in Output Feedback (OFB) mode? If so, what would be the advantage of this?

(c) What is a *one-time key pad*? What are the main advantage and disadvantage of the *one-time key pad*? [6]

Part B

Question 3

(a) Bell-LaPadula is a famous security model designed to provide a secure multi-user operating system.

i. Describe the *no-read up and no-write down* rules enforced in the Bell-LaPadula model. [4]

ii. Explain why strict enforcement of the *no-read up and no-write down* rules could cause a problem for users of the system, and how Bell-LaPadula overcomes this problem. [4]

(b) Distinguish the concept *computational security* from *unconditional security*. Explain why the unconditional security cannot be studied from the viewpoint of the computational complexity. [4]

(c) Use the Fermats little theorem with base 2 as an example to demonstrate that the decimal 93 is not a prime number. [6]

(d) Alice has the RSA public key $(e, n) = (13, 93)$.

i. Encrypt the message $m = 7$ to be sent to Alice. Show all your work. [4]

ii. Show that $d = 37$ is the value of Alice's private key. [4]

iii. Explain how Alice could encrypt and sign a message for Bob. [4]

Question 4

(a) Consider passwords that consist of *three* uppercase followed by *two* lowercase alphabetic characters. Assume that it requires *five* seconds to test such an individual password. Compute the time it would take to find a password in the worst case using exhaust search. Show all your work. Would it be more difficult to guess a password consisting of *four* letters of mixed cases? Justify your answer. [7]

(b) Outline the fast algorithm for modular exponentiation in a flowchart or pseudocode. Use $6^{11} \bmod 13$ as an example to demonstrate how the algorithm works. Trace the values of y, u, and n on each step. [6]

(c) Consider the following scenario.

> Carol uses an archive service company SecureStore to store a large electronic file for her on the company's computer ArchiveBlue. Carol will pay SecureStore for this service. Carol intends to keep a copy of the file herself so the copy on computer ArchiveBlue is a backup, in case her own copy of the file is lost or damaged. SecureStore would like to destroy the file because it takes up a lot of space and is of no value to them. However, they would like to continue to be paid for storing the file. Carol needs to be able to perform some kind of check (as many times, and whenever Carol chooses) to ensure that SecureStore still has the complete version of the file. The file is too large for her to insist on seeing the entire file, instead Carol must use a protocol involving a hash function.

i. Explain why the following protocol does not guarantee that SecureStore still has a copy of the entire file.
Carol asks SecureStore to send her the value of SHA512(file). Carol computes SHA512(file) herself and compares her result with the value sent to her by SecureStore. If these match, Carol accepts that SecureStore still has the file. [5]

ii. The protocol given in part c.(i) works if Carol sends SecureStore a random salt value and asks them to return to Carol the hash of the file concatenated with the salt. It is important that the salt and the file are concatenated in the correct order.
Let "$x \parallel y$" denote the file after concatenation in which content x appears before y. Which of the following values should Carol ask SecureStore to send her? Explain your answer. [7]
(1) $SHA512(file \parallel salt)$
(2) $SHA512(salt \parallel file)$

(d) Demonstrate how a *one-time key pad* of certain length may be generated iteratively without a cycle using the XOR operator $\oplus$ and the initial key 0110. Describe briefly the algorithm that you use. [5]

Question 5

(a) Explain why PGP allows a user to have more than one public or private key pair. Describe how the receiver knows which of the multiple public keys is operational in encryption and authentication. [7]

(b) Alice and Bob want to use the Diffie-Hellman Key exchange protocol to generate a shared secret key. They have agreed to use prime number $p = 17$ with generator $g = 3$. Alice chooses secret key $a = 6$ and Bob chooses secret key $b = 11$. What is the value of their shared secret key? Show all of your work. [6]

(c) Demonstrate your knowledge by commenting on each of the statements below. Explain why you agree or disagree with the conceptions. [9]

i. Public-key encryption is more secure from cryptanalysis than conventional encryption.
ii. Public-key encryption is a general-purpose technique that has made conventional encryption obsolete.
iii. The key distribution is easier when using public-key encryption, compared to the rather cumbersome hand shaking involved with key distribution centres for conventional encryption.

(d) 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. [8]

Name	Sex	Race	Loans	Fines	Drugs	Address