THIS PAPER IS NOT TO BE REMOVED FROM THE EXAMINATION HALLS

UNIVERSITY OF LONDON **CO3326 ZA**

BSc Examination

COMPUTING AND INFORMATION SYSTEMS, CREATIVE COMPUTING AND COMBINED DEGREE SCHEME

Computer Security

Date and Time: Thursday 5 May 2016: 10.00–12.15

Duration: 2 hours 15 minutes

There are FIVE questions in this paper. Candidates should answer **THREE** questions. All questions carry equal marks, and full marks can be obtained for complete answers to a total of **THREE** questions. The marks for each part of a question are indicated at the end of the part in [.] brackets.

Only your first THREE answers, in the order that they appear in your answer book, will be marked.

There are 75 marks available on this paper.

A hand held calculator may be used when answering questions on this paper but it must not be pre-programmed or able to display graphics text or algebraic equations. The make and type of machine must be stated clearly on the front cover of the answer book.

Question 1

(a) 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]

(b) 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.

(c) Write the missing words or phrases 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.

(d) Write the missing words or phrases 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)__.

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

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

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

Question 2

(a) Consider designing a distributed multi-user security system where access control on documents is to be applied. Discuss the advantages and disadvantages of the centralised security that is controlled by the system manager. Justify your answer. [5]

(b) 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]

(c) 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?

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

Question 3

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

(b) Describe two properties that are required for a one-way function. Demonstrate how password files can be protected by one-way functions. [10]

(c) Suppose in a particular implementation it takes $10\mu s$ to do a modular multiplication when the number of operand bits $b = 100$. Approximately how long would it take to do a modular multiplication when $b = 200$? [5]

(d) Draw a diagram to demonstrate the hierarchy of the object sensitivities of a *Military Security Policy* using the security *Protection Ring* model, including the names of the five security levels for the corresponding sensitivities. [5]

Question 4

(a) 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 $h(k) = k \bmod 11$. Assume the hash table is empty initially, demonstrate the hash codes in the table. [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.

> Amenda uses an archive service company FileArchi to store a large electronic file for her on the company's computer Backen. Amenda will pay FileArchi for this service. Amenda intends to keep a copy of the file herself so the copy on computer Backen is a backup, in case her own copy of the file is lost or damaged. FileArchi 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. Amenda needs to be able to perform some kind of check (as many times, and whenever Amenda chooses) to ensure that FileArchi still has the complete version of the file. The file is too large for her to insist on seeing the entire file, instead Amenda must use a protocol involving a hash function.

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

ii. The protocol given in part c.(i) works if Amenda sends FileArchi a random salt value and asks them to return to Amenda 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 Amenda ask FileArchi to send her? Explain your answer. [7]
(1) $SHA512(file \parallel salt)$
(2) $SHA512(salt \parallel file)$

Question 5

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

(b) Bob has a public RSA key $(n = 77, e = 13)$. He sends Alice a message m and the digital signature s of the message. The message and signature that Alice receives is $(m = 3, s = 5)$. Should Alice accept the message as genuine or not? Give justification for your answer. [5]

(c) Describe the X.509 certification process: [6]

i. detailing how the Certification Authority provides a certificate for a user (Bob).
ii. explaining how another user (Alice) can verify that she has the public key of Bob.

(d) In the context of authentication, define and describe the following threats: [10]

i. password guessing
ii. password spoofing
iii. reading password files

END OF PAPER