

THIS PAPER IS NOT TO BE REMOVED FROM THE EXAMINATION HALLS
--

UNIVERSITY OF LONDON

CO3326 ZB

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.

© University of London 2016

Question 1

- (a) Write the missing words, phrases, or sentences onto your answer book to form a truth statement: [5]
- i. A shift cipher such as Caesar's cipher is easy to be broken because (1) . For example, (2) .
 - ii. A well designed block cipher should have a (3) to prevent statistical analysis attacks, and a (4) to prevent exhaustive search attacks.
- (b) The cipher text "WKLV PHVVDJH LV QRW WRR KDUG WR EUHDN" was produced using a Caesar cipher on a message consisting of only the uppercase English letters plus a 'blank' character which was translated to itself. Demonstrate how clues from the ciphertext can be used to determine the shift value and recover the plaintext. Briefly explain your approach and show all your work. [8]
- (c) Consider the general assets in each of the cases below. Assign a relatively appropriate impact level (low, moderate, or high) for each of the potential losses in confidentiality, availability and integrity. Justify your answers. [7]
- i. An organisation managing public information on its Web server
 - ii. A financial organisation managing routine administrative information (not privacy-related)
 - iii. An electrical power supplier containing some supervisory control and a data acquisition system controlling the distribution of the electric power for a large military installation.
- (d) Demonstrate how to compute 2^{15} with the minimum number of multiplications. Show all your work. [5]

Question 2

- (a) Suppose in a particular implementation it takes $20\mu s$ 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]
- (b) Consider designing a distributed multi-user security system that applies access controls on documents. Discuss the advantages and disadvantages of allowing the access to documents to be controlled by each user. Justify your answer. [5]
- (c) Consider the essential properties of a cryptographically strong hash function $y = H(x)$. Two of the properties are
- i. x must be allowed to be of any length
 - ii. Given y , it should be hard to derive x .
- Describe two other essential properties, and explain why these two other properties are required. [5]
- (d) 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. [4]
- (e) Explain what is meant by *symmetric* encryption. List four purposes for which symmetric encryption is especially appropriate. [6]

Question 3

- (a) Bell-LaPadula is a famous security model designed to provide a secure multi-user operating system. Write the missing words or phrases onto your answer book to form truth statements. [8]
- i. The following statements are about *no-read up and no-write down* rules enforced in the Bell-LaPadula model.
Every subject is (1) _____. Every object is (2) _____. A subject can only (3) _____. To prevent objects being copied from a higher level to a lower level, there is also a (4) _____.
- ii. The following statements are about **why strict enforcement** of the *no-read up and no-write down* rules could cause a problem for users, and how Bell-LaPadula overcomes this problem.
The no-read up and no-write down policies mean that (5) _____. A subject at a higher level cannot (6) _____. To overcome these problems, BLP allows (7) _____. It also allows a set of trusted subjects to (8) _____.
- (b) Alice and Bob want to use the Diffie-Hellman Key Exchange protocol to generate a shared secret key k . They have agreed to use $p = 19$ with $g = 3$. Alice chooses secret key $a = 4$ and Bob chooses secret key $b = 5$.
- i. Demonstrate, step by step, how k is devised and shared between Alice and Bob. What is the value of their shared secret key? Show all of your work. [6]
- ii. Explain and demonstrate how Charles could corrupt the Diffie-Hellman Key Exchange protocol and get the secret key himself. Assume $c = 2$. [6]
- (c) Derive the access control table for a system with the following requirements: [5]
- i. User Catherine has read and write access to `windows.exe` and has read, write and execute access to `report.doc`.
- ii. User Branda has read access to `windows.exe` and `citynight.jpg`.
- iii. User Alice has execute and read access to `report.doc` and read access to `election.ps`.
- iv. User Dan has a full access to all the files.

Question 4

- (a) Describe how PGP provides simultaneously confidentiality, authentication and compression. [14]

Your answer should describe

- i. how a user compresses, digitally signs and encrypts a message
- ii. how the receiver determines the original message and authenticates.

It is not necessary to give specific details about particular hash functions, symmetric cryptosystems and public key cryptosystems.

- (b) Name two other services that PGP offers. [2]

- (c) Consider the key generation of a RSA public-key cryptosystem in which $n = 115$.

- i. Explain which value, $e = 12$ or $e = 15$, is usable to generate a public key. Justify your answer. [5]

- ii. What is the value of the public key? [1]

- iii. Compute the corresponding private key for the usable e . [3]

Show all your work.

Question 5

- (a) Describe the *discrete logarithm problem* (DLP) as a one-way function. Use the values $g = 2$, $p = 13$ and $x = 7$ as an example to aid your description and to demonstrate your understanding. [5]
- (b) Alice would like to receive a secret message $m = 5$ from Bob using the El Gamal public key encryption scheme. She was advised to set up keys first and was given the following algorithm to generate her keys:

- (1) Choose a prime number p
- (2) Choose a random number g (less than p)
- (3) Choose a random number a (less than p)
- (4) Compute $y = g^a \bmod p$.

Following the advice, Alice chose $p = 11$, $g = 3$, $a = 8$, but was told later by her friend that both the given algorithm and her chosen values are flawed.

- i. Identify the errors in the key-generation algorithm and write your corrections. [3]
 - ii. Explain which value chosen by Alice is wrong. Suggest a correct value for Alice. Justify your answer and show all your work. [5]
 - iii. Determine y . Write the public key and private key. [2]
 - iv. Bob now can encrypt the (short) message $m = 5$. Assume Bob chooses $k = 9$. Devise the *ciphertext*(m). [4]
- (c) 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? [6]

END OF PAPER