CM2025

BSc EXAMINATION

COMPUTER SCIENCE

Computer Security

Release date: Monday 14 March 2022 at 12:00 midday Greenwich Mean Time

Submission date: Tuesday 15 March 2022 by 12:00 midday Greenwich Mean Time

Time allowed: 24 hours to submit

INSTRUCTIONS TO CANDIDATES:

Section A of this assessment paper consists of a set of **TEN** Multiple Choice Questions (MCQs) which you will take separately from this paper. You should attempt to answer **ALL** the questions in Section A. The maximum mark for Section A is 40.

Section A will be completed online on the VLE. You may choose to access the MCQs at any time following the release of the paper, but once you have accessed the MCQs you must submit your answers before the deadline or within **4 hours** of starting whichever occurs first.

Section B of this assessment paper is an online assessment to be completed within the same 24-hour window as Section A. We anticipate that approximately **1 hour** is sufficient for you to answer Section B. Candidates must answer **TWO** out of the THREE questions in Section B. The maximum mark for Section B is 60.

You may use any calculator for any appropriate calculations, but you may not use computer software to obtain solutions. Credit will only be given if all workings are shown.

You should complete **Section B** of this paper and submit your answers as **one document**, if possible, in Microsoft Word or a PDF to the appropriate area on the VLE. Your answers must have your **candidate number** written clearly at the top of the page before you upload your work. Do not write your name anywhere in your answers.

© University of London 2022

SECTION A

Candidates should answer the **TEN** Multiple Choice Questions (MCQs) quiz, **Question 1** in Section A on the VLE.

SECTION B

Candidates should answer any **TWO** questions from Section B.

Question 2

(a) What is meant by containerisation? [2]

(b) Describe **TWO** main benefits of containerisation for software developers. [3]

(c) In the context of adopting open-source libraries:

i. What is the main security risk that should be considered? [2]

ii. What analysis can be conducted for evaluating the security impacts? [3]

(d) Static analysis is the analysis of non-running systems by auditing their code and features. When should static analysis be conducted? [2]

(e) It is common for web services to be deployed on containerised systems. Describe each of the four main attacks described in the Computer Security module that can happen in a containerised system. [6]

(f) Describe how the *two-phase commit* protocol works in distributed database systems. [6]

(g) Businesses and government agencies collect and store large volumes of information about customers, suppliers, distributors, and employees.

i. Who should own this information?

ii. Who should be allowed to access this information?

iii. Should this information be sold to others?

Discuss your opinions or explain difficult issues in answering these questions. [6]

Question 3

(a) What is the so-called DDoS attack in the context of network security? Describe, step by step, how a typical DDoS attack works. [8]

(b) 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? [2]

iii. Compute the corresponding private key for the usable e. [5]

Show all your workings.

(c) 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. [10]

Question 4

(a) Consider each of the scenarios below and write down your own advice, as a security expert to the general public, on what to do in each of the situations. Justify your answers, and, if necessary, add assumptions to ease your discussion.

i. You received an urgent request from your line manager who lost their login password at an important overseas conference and they are asking you for the password. [4]

ii. You have to send one password to a remote site. [4]

(b) Briefly explain the **four** primary attacks to blockchains by hackers and fraudsters? [4]

(c) What is so-called *X-Force Red Blockchain Testing*? [4]

(d) Explain what is so-called *51% attack* in the context of blockchain. [4]

(e) Describe an ideal infrastructure for a private blockchain with integrated security. [5]

(f) Describe **five** applications other than cryptocurrency for blockchains. [5]

END OF PAPER