UNIVERSITY OF LONDON

CM2025

BSc EXAMINATION

COMPUTER SCIENCE

Computer Security

Release date: Thursday 16 March 2023 at 12:00 midday Greenwich Mean Time

Submission date: Friday 17 March 2023 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**.

Calculators are not permitted in this examination. 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. You are permitted to upload 30 documents. However, we advise you to upload as few documents as possible. Each file uploaded must be accompanied by a coversheet containing your **candidate number**. In addition, 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.

UL23/0213

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) Why is designing truly secure systems difficult? State TWO reasons.

(4 marks)

(b) In the context of network security, what are Dictionary and Reply attacks?

(4 marks)

(c) Explain how do Intrusion Detection Systems (IDS) work?

(4 marks)

(d) What is containerization? Explain what are the FOUR container attack routes?

(6 marks)

(e) In the context of security, state ONE positive and ONE negative point about using open-source libraries.

(4 marks)

(f) One of the secure solutions to store passwords in a database is storing their hashed value instead of plain text. However, it is possible to find out which users have the same passwords by checking the hashed values. Propose a solution to avoid this problem while still using cryptographic hash functions. Explain how the passwords should be stored using your proposed solution and how they should be checked.

(4 marks)

(g) Explain how can we check a file is intact using cryptographic hash functions?

(4 marks)

Question 3

(a) Based on the RSA algorithm, answer the following questions:

i. Assume Alice has chosen 13 and 17 as two prime numbers (p and q), thus N=p.q=221. Define a value for e as her public key. Show your work step-by-step.

(4 marks)

ii. For the question in part a i), using the selected value for e, define a private key d. Show your work step-by-step.

(4 marks)

iii. Briefly explain do you recommend a small or a large value among all possible values for e and d while using RSA algorithm? Why? Explain your reasons.

(4 marks)

iv. Assume Bob has chosen the pair (N=143, e=5) as his public key. He is trying to find a private key, but with no success. Why is he unable to find a private key? What is the problem?

(4 marks)

(b) Why are asymmetric cryptographic algorithms more secure than symmetric algorithms? State TWO reasons.

(4 marks)

(c) Using the Playfair cypher algorithm, encrypt the message “COMPUTERSECURITYEXAM”. Consider your first name as the key. Show your work step-by-step.

(10 marks)

Question 4

(a) In the context of blockchain technology, answer the following questions:

i. What is a digital signature? Assume Bob has created a transaction to send some money to Alice. Why should Bob put his digital signature along with his public key inside the transaction?

(6 marks)

ii. What is double spending? How it can be detected and prevented in a blockchain?

(4 marks)

iii. What is the 51% attack? How does it work?

(4 marks)

iv. Explain how malicious nodes (inside the blockchain's peer-to-peer network) are prevented from tampering with transactions using cryptographic hash functions. Assume each transaction contains the digital signature as well.

(4 marks)

v. Name and describe TWO applications other than cryptocurrency for blockchain.

(2 marks)

vi. What does the immutability of the blockchain mean?

(2 marks)

(b) Assume Bob has designed a hash function as follows: His function gets the data to be hashed. Then, he flips a coin 256 times, so he generates a string of Hs (Heads) and Ts (Tails). He replaces H with 1 and T with 0. After that, he writes the data along with the generated binary string which is 256 bits long in a database. Next time, his function searches the data first. If it finds the data inside the database, it immediately returns its binary string, otherwise, it will repeat the process of flipping the coin. Based on the different features that a cryptographic hash function should have [3 marks], explain if this function is a proper hash function or not [2 marks]? Examine at least THREE features [3 marks].

(8 marks)

END OF PAPER