UNIVERSITY OF LONDON

CM2025

BSc EXAMINATION

COMPUTER SCIENCE

Computer Security

Release date: Tuesday 14 September 2021 at 12:00 midday British Summer Time

Submission date: Wednesday 15 September 2021 by 12:00 midday British Summer Time

Time allowed: 24 hours to submit

INSTRUCTIONS TO CANDIDATES:

Section A of this assessment paper consists of a set of **10** 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.

SECTION B

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

Question 2

This question is about Symmetric and Asymmetric Cryptography

(a) What is the difference between symmetric and asymmetric cryptography? Give an example of each.

[2]

(b) Alice and Bob both have private keys and public keys. How can Alice send Bob a message that only he can read? Explain your answer

[4]

(c) Alice and Bob both have private keys and public keys. How can Alice send Bob a message in a way that assures Bob that the message came from Alice. Explain your answer.

[4]

(d) We have the following encoding system: To encode a message you square it. How do you decode a message? What are the merits and drawbacks of this system.

[3]

(e) We make the code in part d a bit more robust by the following scheme: Alice has a private key, which is a number, x. She encodes a message by raising it to the x power. She does not tell anybody what x is but she publishes a decoding function. Explain ways that this is better than the code in d but say why it is still inadequate.

[4]

(f) You are going to encrypt a message uing a playfair code. Make the playfair tableau using *compsecexam* as the key

[5]

(g) Encode the phrase: *This is my message* using the playfair tableau from the previous answer.

[8]

Question 3

This question is about hashing and Cryptographic Hash Functions

(a) What is a hash function?

[2]

(b) A data item in your collection consists of data about a book: title, author, year of publication. Assume that the hash function is H(key) = n mod 100.

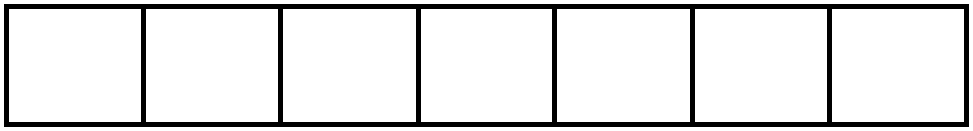
a. Give two reasons why the alphabetical position if the first letter of the title is not a good way to calculate a key.

[4]

b. Suggest a better way to calculate a key and say what is good about it.

[2]

(c) We have the following hash function: H(n) = n mod 7. And you wish to hash data with the following keys: 50, 16, 25, 6. Fill in a picture like below with this data. The first box represents a hash value of 0 etc.



[2]

(d) Explain two strategies for dealing with the next input if it has a hash value of 22.

[4]

(e) Describe how a search function would look for data with each of your strategies

[4]

(f) Look up the following properties of a cryptographic hash function on the internet or elsewhere: Collision resistance, hiding, and puzzle friendliness. Give a careful formal definition. This could be copied, if so, make it clear where it is from. Then in your own words explain what each of the properties means and why it is an important property to ensure security.

[9]

(g) Why is $H(n) = mmod100$ a poor choice for a cryptographic hash function?

[3]

Question 4

This question is about secure development and deployment

You are working on some new software for the touch screen system that sells tickets in train stations. The system consists of a set of networked computers in the station which communicate with a

(a) "Secure software development is not all about coding". Justify this statement with TWO other aspects of secure software development that do not involve coding.

[4]

(b) The ticket machine in the station will run a Linux operating system. Describe TWO methods you would use to analyse the default security of the operating system.

[4]

(c) The sales manager has explained to the train company that your system will use "not one but three totally different types of firewall to maximise the secure experience of customers". Is this a reasonable statement? Explain your answer.

[3]

(d) The sales manager has been reading more internet articles about security and has promised that the ticket selling system will use "un-hackable containerisation" on the server side. Describe THREE ways in which containerised systems are vulnerable.

[6]

(e) You decide to use the python language. Name a tool that you can use in Python to audit third-party libraries

[1]

(f) Does the auditing tool you mentioned carry out passive or dynamic analysis? Justify your answer.

[2]

(g) The sales manager has informed the client for the project that you will be using blockchain technology to ensure that the person buying the ticket is the only person that can use that ticket. Explain in some detail how you would go about using blockchain technology to achieve this. Consider the following problems: how would you identify the person, how would you represent a ticket on the blockchain? how would you connect that identity to a given ticket? How might a ticket inspector establish if the person on the train is the person who owns the ticket?

[10]

END OF PAPER