UNIVERSITY OF LONDON

CM2025

BSc EXAMINATION

COMPUTER SCIENCE

Computer Security

Release date: Friday 26 March 2021 at 12 midday Greenwich Mean Time

Submission date: Saturday 27 March 2021 by 12 midday Greenwich Mean Time

Time allowed: 24 hours to submit

INSTRUCTIONS TO CANDIDATES:

Section A of this assessment 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 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 from Section B.

Question 1

You are part of the team working on some new web services for a company. In the following questions, you are going to apply your knowledge of computer security principles to improve the security of the web services.

(a) It is common for web services to be deployed on containerised systems. State the source and target of the four main attacks that can happen in a containerised system. [4]

(b) The team developing the web services is considering using an open source python framework. You want to assess the security of the library before using it.

i. What is static analysis? [1]

ii. Do you think static analysis is suitable for evaluating the security of the framework? Explain why. [3]

(c) What is the name of the analysis method which evaluates the security of a running system? [1]

(d) You need to store passwords for users somewhere. You are considering symmetric and asymmetric encrytion techniques.

i. Define symmetric encrytion [2]

ii. Define asymmetric encrytion. [2]

(e) Would you use symmetric or asymmetric encrytion to encrypt the passwords prior to storage? Justify your answer. [3]

(f) Explain how a bad actor could go about decrypting the passwords, assuming they had access to the encrypted passwords. [4]

(g) Identify one other element of the attack surface presented by a web service. [2]

(h) How would you go about securing the element you identifed in the previous question from attack? [3]

(i) Describe how you could include security practice in the software development lifecycle. [5]

Question 2

The kid-RSA algorithm is a simplified version of the RSA algorithm. Kid-RSA takes as its input four numbers a, b, a1, b1. The four numbers are converted into four values M, e, d and n, according to the following equations:

M = a * b - 1
e = a1 * M + a
d = b1 * M + b
n = (e * d) / M

A plaintext message P can be encrypted to an encrypted message C with the public key (n,e) using:

C = e * P (mod n).

Once encrypted, C can be converted back to P using the private key 'd' as follows:

P = C * d (mod n)

(a) If a = 123, b = 456, a1 = 789 and b1 = 1234, calculate M, e, d and n. Show your working. [2]

(b) State the public key for these values of a,b,a1 and b1. [2]

(c) Encrypt the message 'Caesar++' using the public key. Show your working. [4]

(d) Decrypt the message. Show your working. [4]

(e) What is the Caeser cipher? What is the category of encryption algorithm that it falls into? [2]

(f) Explain how the Caesar cipher works, using examples. [4]

(g) How would you go about cracking the Caesar cipher? Explain a step by step process that you could use to crack the Caesar cipher. [4]

(h) Compare the Caesar cipher to Kid-RSA. Draw a table wherein you compare FOUR features of the algorithms. [4]

(i) Which of the two algorithms would you recommend if Caesar was alive today? State TWO reasons why you would recommend it. [4]

Question 3

(a) List FOUR core functional components of the infrastructure required to run a blockchain such as bitcoin. [4]

(b) For each of the FOUR blockchain components you listed in the previous question, describe what it does. [4]

(c) Explain how bitcoin removes the need for a central banker role. [4]

(d) Name TWO problems that bitcoin's design solves. [2]

(e) Explain how bitcoin's design prevents the TWO problems you mentioned in the previous question from occurring. [4]

(f) Describe a bitcoin transaction. What data is contained therein? [3]

(g) There has been some interesting research into the use of blockchains in education contexts. Reflecting on your experience of education systems, come up with an idea for how blockchain technology could be used in an education context. Consider things like exams, degree award certificates and so forth.

i. Describe the example application of blockchain to the educational domain that you have in mind. [2]

ii. Explain how it makes use of data on the blockchain. [3]

iii. State how it makes use of smart contracts or other data processing on the blockchain. [4]

END OF PAPER

.