UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

Department of Computing

B. Sc. Examination 2019

IS53012B
Computer Security

Duration: 2 hours 15 minutes

Date and time:

This paper is in two parts: part A and part B. You should answer ALL questions from part A and TWO questions from part B. Part A carries 40 marks, and each question from part B carries 30 marks. The marks for each part of a question are indicated at the end of the part in [.] brackets.

There are 100 marks available on this paper.

Electronic calculators must not be programmed prior to the examination. Calculators which display graphics, text or algebraic equations are not allowed.

**THIS PAPER MUST NOT BE REMOVED
FROM THE EXAMINATION ROOM**

Part A

Question 1 Parts (a)–(i) require answers True or False with justifications. You should read each statement carefully and then determine whether the statement is TRUE or FALSE. If the statement is true, explain why it is true or give a supportive example. If it is false, give the correct answer or provide a counterexample.

(a) A *security model* is a means for formally expressing the rules of the security policy in an abstract way. [5]

(b) A cryptosystem is defined to be *conditionally secure* if the system can be broken with infinite computations resources.

(c) A vulnerability is a potential to do harm. A control is a means by which a threat agent can cause harm. A threat is a protective measure that prevents a threat agent from exercising a vulnerability. [5]

(d) The product of two relatively simple ciphers, such as a *substitution* and a *transposition*, can achieve a high degree of security. This is because that ideally a substitution cipher contributes to the diffusion property where as a transposition cipher to the confusion property. [5]

(e) In mathematics terms, a one-way function is a function $f : X \to Y$, i.e. $y = f(x)$, such that [5]

- Given $x \in X$, it is easy to compute $y = f(x) \in Y$
- but given $y \in Y$, it is difficult to find an $x \in X$ such that $y = f(x)$.

(f) The system of all subsets of a finite set, under the operation *subset of* ($\subseteq$), does not form a lattice. [5]

(g) A well designed block cipher should have a large blocksize (alphabet size) to prevent statistical analysis attacks, and a large keysize to prevent exhaustive search attacks. [5]

(h) The traditional authentication methods are unsuitable for use in computer networks mainly because they do not permit high speed data flow. [5]

(i) The advantage of the Rivest, Shamir, Adelman (RSA) public key system over the Digital Signature Algorithm (DSA) is that it uses the secure hash algorithm to condense a message before signing. [5]

Part B

Question 2

(a) 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 her secret key $a = 4$ and Bob chooses his secret key $b = 5$.

i. Demonstrate, step by step, how the secret key k is devised and shared between Alice and Bob. What is the value of k? Show all your work. [6]

ii. Explain and demonstrate how Charles can corrupt the Diffie-Hellman Key Exchange system by getting the secret key k himself. Use the data in part a.(i) as an example and assume Charles has a private key $c = 2$. [6]

(b) Consider the college database system FS that would answer the normal statistical queries such as TOTAL and LIST for each department. Two news reporters John and Lisa are both granted access to FS as visitors. John and Lisa later divide the coverage responsibilities between themselves and each concentrates on reporting the news of one department.

i. Discuss the sensitivity of each of the disclosures (1)–(3) below from FS's viewpoint, and explain why it does or does not cause concerns in the context of confidentiality. Add assumptions if necessary to ease your discussions. [9]

(1) John queries the total of the financial supports received by students in his department.

(2) Lisa queries the name list of the students receiving financial supports in her department.

(3) John queries the *total* of the financial supports received by students in his department, and the *list* of the students receiving financial supports in the department.

ii. What computation would the database management system of FS have to perform in order to determine that the list of student names might reveal sensitive data? [3]

(c) Demonstrate how a *one-time key pad* of certain length may be generated iteratively without a cycle using the XOR operator $\oplus$ and the initial key 0110. Describe briefly the algorithm that you use. [6]

Question 3

(a) Examine the correctness of the statements below regarding what firewalls can or cannot do. For each statement, state TRUE if you agree or FALSE otherwise. Rewrite each false claim to transform it to a true statement. Justify your answers. [13]

i. Firewalls can protect an environment only if the firewalls control the entire premises.
ii. Firewalls can protect data near the premises.
iii. Data that have properly passed through the firewalls are safe.
iv. Firewalls are the most visible part of an installation to the outside so they are more attractive targets of attacks.
v. Firewalls must be correctly configured, updated, and reviewed periodically.
vi. Firewalls are impenetrable. The smaller, the better.
vii. Firewalls exercise only minor control over the content admitted to the insider.

(b) Describe, with the aid of a diagram, what concurrent modification problems may occur in a multi-agent airline booking system. Using the *two-step commit* approach, describe how to avoid assigning one seat to two people. List precisely which steps the database manager should follow in assigning passengers to seats. Describe your assumptions using a diagram. [10]

(c) Explain what it is meant by a *generator for prime p* when the discrete logarithm problem is discussed for a cryptographic protocol. Demonstrate why 2 is not a generator for prime 7. [7]

Question 4

(a) Software Auditing involves a process of analysing software codes to uncover vulnerabilities. Consider the table below which summarises various types of program source code auditing. Interpret and explain the contents presented in the table to demonstrate your knowledge. [8]

	in-house	third party	independent
prerelease software	√		
postrelease software	√		
product range comparison		√	
preliminary evaluation		√	
evaluation		√	
research			√

(b) Assume that Alice would like to encrypt a document m 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 values chosen by Alice are wrong. Suggest correct values for Alice. Justify your answers and show all your work. [Note: You should give the smallest possible value if there are a number of correct values] [9]

iii. Determine y. Write the public key and private key. [2]

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