UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

Department of Computing

B. Sc. Examination 2018

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)–(g) require true or false answers 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, explain what the correct answer should be.

(a) Access control matrices can represent anything that is represented by access control lists.
True or False? Justify your answer concisely. [4]

(b) If the sender and receiver use different keys, the system is referred to as conventional cipher system.
True or False? Justify your answer concisely. [4]

(c) Having generated a RSA public and private key pair, and published the public key, John can conclude that is all he needs to be able to send you a securely encrypted email.
True or False? Justify your answer concisely. [4]

(d) If Emma Intelligent tomorrow discovers an efficient algorithm for computing the greatest common divisor of two extremely large numbers, this will make it possible to break RSA.
True or False? Justify your answer concisely. [4]

(e) In the RSA algorithm, we select 2 random large values p and q. p and q should be co-prime.
True or False? Justify your answer concisely. [4]

(f) In the RSA algorithm, $\phi(n)$ should be $(p+1)(q+1)$.
True or False? Justify your answer concisely. [4]

(g) Consider data that is stored over time in a mandatory access control based system. The contents of files containing highly classified ("top secret") information are necessarily more trustworthy than material stored in files marked unclassified.
True or False? Justify your answer concisely. [4]

(h) Concisely describe two fundamentally different approaches for user authentication. [4]

(i) Explain, from the point of view of a cryptanalyst, the use of *entropy* of a piece of message in the context of Computer Security. Give an example to demonstrate how the entropy can be calculated. [4]

(j) The following statements are about shift ciphers. Write the missing words, phrases, or sentences into your answer book to form truth statements: [4]

i. A shift cipher such as Caesar's cipher is easy to be broken because ____(1)____.
For example, ____(2)____.

ii. A well designed block cipher should have a ____(3)____ to prevent statistical analysis attacks, and a ____(4)____ to prevent exhaustive search attacks.

Part B

Question 2

(a) Security systems based on lattices are common. Explain what is a lattice by describing its two properties. Consider the system of all subsets of a finite set (A, B, C) under the operation 'proper subset of' ($\subset$). Does this system form a lattice? Why or why not? Draw the lattice if Yes, and modify the operation otherwise so a lattice may be formed. [8]

(b) When shopping at Costco in the USA, after you have selected your purchases you take your shopping trolley full of goods to one of the registers. The check-out clerk scans your goods, totals what you owe, and upon receiving payment from you gives you an itemised receipt. However, you cannot then simply leave the building with your goods. At the exit you are required to stop by a staff member who inspects your receipt. If the receipt looks OK (e.g. appears to match the number and types of items in your trolley), the staff member draws a line with a permanent marker down the receipt and hands it back to you. At this point, you can exit the building and take the goods to your car and go home.

i. Identify and explain two security principles illustrated by Costcos approach. For each, describe concisely what aspect of Costcos approach reflects the security principle. [15]

ii. Identify an attack that Costco seeks to prevent by having the staff member draw the line down your receipt. Describe concisely how the attack works. [7]

Question 3

(a) Explain, with the aid of an example, what a *boundary condition violation error* is in the context of software security. [7]

(b) Explain what is meant by the "n-item k-percent rule" in the context of database security. Use the example table below to aid your explanation and demonstrate your view points. Add assumptions if necessary. [10]

	Loring	Surrey	Dean	Total
Male	1	3	1	5
Female	2	1	3	6
Total	3	4	4	11

(c) In an RSA system the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user? Justify your answer and show all your work. [13]

Question 4

(a) Discuss what makes a network vulnerable to attacks. Justify your answer. [8]

(b) Consider a supermarket website that includes the notion of a "shopping trolley". Customers visiting the site put items of interest in their shopping trolley. After finishing their browsing and shopping, they click on Checkout to pay for the items. At that point, the customer logs into the site to enable the site to retrieve their payment information.

i. Suppose that the site implements the shopping trolley by storing the associated items and prices in files on the server, with one file for each customer. The site identifies customers by their IP addresses. This design is vulnerable to a DoS attack. Concisely explain the attack by describing what an attacker can do. [8]

ii. Suppose that instead the site keeps a list of shopping trolley items on the client side. Every time a user clicks on "add-to-trolley", the server sends all of the associated details (item name, price, quantity) in its reply, incorporating them into a hidden HTML form field. Through some Javascript magic, now when the user finally clicks on Checkout, all of the previously bought items embedded in the hidden form field are sent to the server. The server then joins them together into a list and presents the user with the corresponding total amount for payment.

- Is this design vulnerable to the DoS attack you described earlier in your answer in part b.(i)? Explain why or why not. [7]
- Is this design secure from other attacks? If so, explain the basis for your claim. If not, describe an attack on it. (You can assume that the site is safe from web attacks such as CSRF, XSS and SQL injection, and uses HTTPS for the Checkout procedure.) [7]