UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

B. Sc. Examination 2015

Computing

IS53012A Computer Security

Duration: 2 hours and 15 minutes

Date and time:

There are five questions in this paper. You should answer no more than three questions. Full marks will be awarded for complete answers to a total of three questions. Each question carries 25 marks. The marks for each part of a question are indicated at the end of the part in [.] *brackets.*

There are 75 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

Question 1

(a) Consider the RSA (Rivest, Shamir and Adleman) cryptosystem. Before sending a message $m = 3$ to Alice, Bob prepares his keys carefully. He randomly chooses $p = 5$, $q = 7$ and $e = 7$. Answer the following questions on the RSA. Show all your work. [6]

i. What is the value of $r = \varphi(n)$?
ii. Which value is computed using the *Euclid's algorithm*?
iii. Which values are used as Bob's *public key*?

(b) The Education Department of a university consists of two sections: *student* and *staff*. An employee can work for up to both sections, and the documents available are classified as *open* or *private*. A security level is represented by a pair (x, y) where x is either open or private, and y is a subset of the set (student, staff). A security level (x_1, y_1) dominates the security level (x_2, y_2) if $x_1 = x_2$ or if x_1 is private and x_2 is open, and if y_2 is a subset of y_1. [9]

i. How many security levels are there?
ii. Represent the access control structure by a lattice.
iii. Determine which security level dominates both the security levels (open, (student)) and the security level (private, (staff))

(c) Consider the scenario below. Identify one security misconduct and suggest an appropriate alternative. [6]

The Research Office and Finance Department in a University are working to correct an error in John's bank account due to a direct deposit mistake. The Research Office emails the correct account and deposit information to the Finance Department, which promptly fixes the problem. John confirms with the bank that everything has, indeed, been sorted out.

(d) Consider the descriptions below of four commonly-used security tools (a–d) that, if in place, may protect one's laptop computer from online threats. Identify each of the security tools. [4]

a. would keep the computer and operating system updated with the latest patches.
b. would scan the software system and kill viruses that could disable or destroy the operating system.
c. would look for evidence of malware that would allow others to watch the Internet activity or potentially even take over the system for their own use.
d. would protect the computer by creating a virtual barrier against hackers who can exploit security vulnerabilities to access the computer and steal the information or worse.

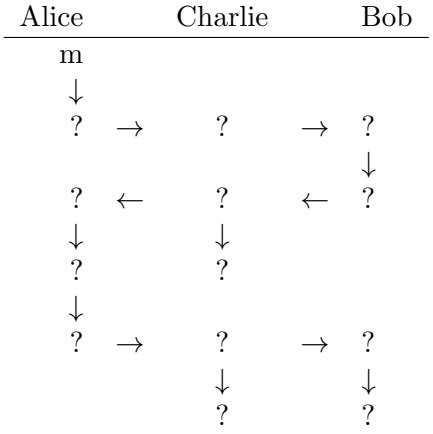
Question 2

(a) Explain, with the aid of an example, which characteristics of a *one-way function* can be useful for cryptography. [6]

(b) Kevin proposes a cryptosystem that requires no key distribution. It works as follows: To send Bob a message m, Alice generates her key a, a sequence of random bits (the same length as m), computes $c = m \oplus a$, where $\oplus$ represents the bitwise XOR operation, and sends c to Bob.
On receipt of c, Bob generates his own random bits b of same length, computes $d = c \oplus b$ and sends d to Alice. On receipt of d, Alice computes $e = d \oplus a$ and sends e to Bob. On receipt of e, Bob computes $f = e \oplus b$ for the last time.

i. Consider an example where $m = 10110$, $a = 11011$ and $b = 01001$. Demonstrate how Bob can get the message m. Show all your work. [2]

ii. Annotate a diagram with logic expressions at each step using the format below. Explain why or why not Kevin's cryptosystem works. [7]



(c) Give a brief step-by-step account of *distributed denial of service* attacks. Comment on the seriousness of these attacks using known statistics data. [6]

(d) Distinguish the concepts *computational security* from *unconditional security*. Explain why the unconditional security cannot be studied from the viewpoint of the computational complexity. [4]

Question 3

(a) 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 1011. Describe briefly the algorithm that you use. [4]

(b) Explain what is the main disadvantage of the *one-time key pad* despite offering perfect secrecy. [2]

(c) Consider the two columns of text below. Three common software flaws are listed in the left column and three error messages in the right column. In the context of program security, pair each of the error messages in the right column with its corresponding flaw name in the left column. Outline the main characteristics of each flaw, and justify your answer with the aid of clues from its matching error message. Add assumptions if necessary to ease your discussions. [12]

1. validation error	A. "Out of range! Please re-enter the data!"
2. domain error	B. "Unexpected element link. The content of the parent element type must match!"
3. serialisation/aliasing error	C. "Incompatible format! The disk forms of Hashtable (older) and HashMap (newer) are different and incompatible!"

(d) Explain, with the aid of an example, the vulnerabilities in *software design*, *implementation* and *operation*. [7]

Question 4

(a) Discuss the general security requirements for databases systems in terms of integrity, confidentiality and availability. [10]

(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 to ease your discussion. [5]

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

(c) 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]

Question 5

(a) Explain what security problem can be solved using *password salting* and how. [5]

(b) Demonstrate how the Vernam cipher works, using the example of
the plaintext "`1110 0110 1110 111`" and
the one-time key pad 1111 0101 1001 000,
applying the *addition modular 2* (XOR) operation. [6]

(c) Consider the two columns of text below. Match each of the network attacks listed in the left column with an applicable description in the right column. Write down the labels of each matching pair.

For example, write "1–J" if the first item (1. ARP spoofing) in the left column matches the last description item (*J. Taking advantage of the impersonated victim's ability to establish a connection with the target victim host*) in the right column. [5]

	A. Sending an oversized ICMP echo request message
1. Fingerprinting	*B. Sending overlapping IP datagram fragments*
	C. Capturing frames in broadcast channels
2. Ping-of-death	*D. Identifying application services running on the potential victim host*
	E. Taking advantage of routers in broadcast mode
3. SYN flooding	*F. Same source and destination IP addresses and same source and destination port numbers*
	G. Redirecting frames to the attackers computer instead of the intended recipient within a LAN
4. Smurf	*H. Determining the specific vendor software and version the potential victim host is running*
5. Sniffing	*I. Taking advantage of the TCP buffer space used during a handshake exchange*
	J. Taking advantage of the impersonated victim's ability to establish a connection with the target victim host

(d) Let p be a large number and let the positive number g have the exponent $p - 1$. Explain why or why not the function $h(x) = g^x \bmod p$ is a one-way function. Give your reasons. [5]

(e) A hash function can be used to produce a fingerprint of a file, a message, or other block of data. To be useful for message authentication, a hash function H must have the property that *for any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$*. Explain what would happen if H does not have this property. You may use an example to illustrate your points. [4]