UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

B. Sc. Examination 2013

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 relative severity of attacks reported in the Computer Crime and Security Survey for 2010/2011 by the US Computer Security Institute (CSI). Rank the nine major categories of attacks below, from the most severe (No.1) to the least severe (No.9), according to the views in the report at the time. Comment on the attack trend in severity (increase, decrease or unchanged) for each category. [6]

(i) Financial fraud, (ii) Password sniffing, (iii) Exploit of wireless networks, (iv) Denial of service, (v) Malware infection, (vi) Bots on network, (vii) Insider abuse of internet access or email, (viii) Phishing, (ix) Laptop/mobile device theft.

(b) Suppose in a particular implementation it takes $20\mu s$ to do a modular multiplication when the number of operand bits $b = 100$. Approximately how long would it take to do a modular multiplication when $b = 200$? [5]

(c) For the assets in each of the cases below, assign an impact level (low, moderate, or high) for each of the potential losses in confidentiality, availability and integrity. Justify your answers. [7]

i. An organisation managing public information on its Web server
ii. A law enforcement organisation managing extremely sensitive investigative information.
iii. A financial organisation managing routine administrative information (not privacy-related)
iv. An information system for large acquisitions in a contracting organisation contains both a) sensitive pre-solicitation phase contract information and b) routing administrative information. Assess the impact for the two data sets separately and the information system as a whole.
v. An electrical power supplier contains supervisory control and a data acquisition system controlling the distribution of the electric power for a large military installation.

(d) Explain how the transposition cipher works. Demonstrate how the plaintext can be decrypted from the ciphertext `HKFPRZNIWUVLG_UOJOEO_TCNMEAOEBOETYCQRXDHDE`, using the key `IAMTHE`. [7]

Question 2

(a) Explain in what situation a hash function on a *fixed length* input is a one-way function and in what situation it is not. Refer to the example below in your explanation.

A message of length m consisting of n segment blocks of lengths, $m_1, m_2, \cdots, m_n$. No block message length is bigger than some integer b, i.e. $0 \leq m_i \leq b$, and $1 \leq i \leq n$. Consider the use of a hash function of $h(m) = m \bmod b$. [6]

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

(c) What is an access control table? Demonstrate an example with two subjects (Jones, Smith) and three file objects (`timetable.doc, install.exe, format.jpg`). Assume standard operations on files. [6]

(d) (Scenario) John proposes a cryptosystem that is based on one-time key pad and it works as follows: If she wants to send Bob a message m, Alice generates her key a, a sequence of random bits (the same length as m), computes $c = m \oplus a$ and sends c to Bob, where $\oplus$ represents the bitwise XOR operation. 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 $e \oplus b$ for the last time.

Annotate a diagram with logic expressions representing the message flow, and hence explain how Bob can finally get the message m in John's cryptosystem. Demonstrate, with the aid of another diagram and logic expressions, how the third person Charlie can also obtain the message m. [8]

Question 3

(a) (Scenario) You are the *Security Manager* of a local school and noticed an instance of system crash on the new IT server. The IT department reported to you later that the system crash was due to an erratic input by a new student and recommended to do nothing.

What would be your view on the recommendation and why? Supposing that you think the instance reflects security vulnerabilities, what is the category of the vulnerabilities often referred to? Explain what are often involved in such vulnerabilities and give examples to illustrate the vulnerabilities. [6]

(b) Describe the *discrete logarithm problem* for modular arithmetic. [5]

(c) Explain what is meant by a trusted operation system. Provide examples to support your explanation. [6]

(d) Examine the correctness of the statements below regarding what firewalls can or cannot do. For each statement, mark a true if you agree or false otherwise. Rewrite each false claim to transform it to a true statement. Justify your answers. [8]

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 to 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.

Question 4

(a) Explain, with the aid of an example, what is meant by *poly-instantiation* in the context of database security. [5]

(b) Explain why encryption is rarely applied to implement separated fields in a database. Discuss both situations where (i) one key is applied to the entire database, and (ii) a different key is applied to each field of the database. [7]

(c) Describe two approaches to control direct statistical inference attacks in database security. [6]

(d) 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. [7]

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

Question 5

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

(b) Describe the X.509 certification process: [6]

i. detailing how the Certification Authority provides a certificate for a user B.
ii. explaining how another user, Alice, can verify that she has the public key of Bob.

(c) Explain how hardware can be designed for fault tolerance. Are these methods applicable to software? Why or why not? [6]

(d) Software Auditing involves a process of analysing software codes to uncover vulnerabilities. The table below summarises various types of program source code auditing.

Interpret and explain the contents presented in the table. [5]

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