UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2011/2012 – 3rd Year Examination – Semester 5

IT5204: Information Systems Security

Structured Question Paper
03rd March, 2012
(TWO HOURS)

To be completed by the candidate

BIT Examination Index No: .....

Important Instructions:

- The duration of the paper is 2 (Two) hours.
- The medium of instruction and questions is English.
- This paper has 4 questions and 11 pages.
- Answer all 4 questions. (all questions do not carry equal marks)
- Question 1 (40% marks) and other questions (20% marks each).
- Write your answers in English using the space provided in this question paper.
- Do not tear off any part of this answer book.
- Under no circumstances may this book, used or unused, be removed from the Examination Hall by a candidate.
- Note that questions appear on both sides of the paper.
  If a page is not printed, please inform the supervisor immediately.
- **Non-programmable Calculators may be used**

Questions Answered

Indicate by a cross (×), (e.g. [X]) the numbers of the questions answered.

	Question numbers				
To be completed by the candidate by marking a cross (×).	1	2	3	4	
To be completed by the examiners:					

1) **Answer each question as true or false, and then justify it, in at most one sentence.**

(a) According to Shannon, the size of enciphered text should be larger than the text of the original message.

(02 marks)

ANSWER IN THIS BOX

(b) The Vernam Cipher is an example of a block cipher.

(02 marks)

ANSWER IN THIS BOX

(c) The Advanced Encryption Standard (AES) algorithm can use three (3) different key sizes.

(02 marks)

ANSWER IN THIS BOX

(d) A symmetric key system with ten (10) users requires 256 keys and each user must track and remember a key for each other user with which he or she wants to communicate.

(02 marks)

ANSWER IN THIS BOX

(e) The Euclidean algorithm is a procedure for computing the greatest common divisor of two numbers.

(02 marks)

ANSWER IN THIS BOX

(f) A Host-based Intruder Detection System (HIDS) is a stand-alone device attached to the network to monitor traffic throughout that network.

(02 marks)

ANSWER IN THIS BOX

(g) PGP uses hierarchically validated certificates, usually represented in X.509 format, for key exchange.

(02 marks)

ANSWER IN THIS BOX

(h) Integrity means that customers or partners can be held accountable for transactions, such as online purchases, which they cannot later deny.

(02 marks)

ANSWER IN THIS BOX

(i) A firewall is a device that keeps certain kinds of network traffic out of a private network.

(02 marks)

ANSWER IN THIS BOX

(j) Organizations can use dictionaries to screen passwords during the reset process and thus guard against the use of easy-to-guess passwords.

(02 marks)

ANSWER IN THIS BOX

(k) Popular cryptographic protocols use a hybrid combination of symmetric and asymmetric algorithms.

(02 marks)

ANSWER IN THIS BOX

(l) A logic bomb is a class of malicious code that executes various commands sent by a remote attacker.

(02 marks)

ANSWER IN THIS BOX

(m) The greatest common divisor of 123309 and 9315 is 27.

(02 marks)

ANSWER IN THIS BOX

(n) A patent protects the expression of an idea and a copyright protects an invention.

(02 mark)

ANSWER IN THIS BOX

(o) (18, 17), (8,3), (16,21) are relatively prime numbers.

(02 mark)

ANSWER IN THIS BOX

(p) The Digital Signature Algorithm (DSA) can be used for signing and encryption.

(02 mark)

ANSWER IN THIS BOX

(q) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points, A and B and have chosen integer value 3 as g and the integer value 10 as n. If A generates the private key x=5 and B generates the private key y=6, the session key k between A and B is 9.

(02 mark)

ANSWER IN THIS BOX

(r) The Kerberos authentication protocol requires two systems, called the Certification Authority (CA) and the Digital Certificate (DC), which are both part of the Key Distribution Center (KDC).

(02 mark)

ANSWER IN THIS BOX

(s) Discretionary access control (DAC) means that access control policy decisions are made beyond the control of the individual owner of an object.

(02 mark)

ANSWER IN THIS BOX

(t) The Bell and La Padula security model is a formalization of military security policy and was central to the U.S. Department of Defence's Trusted Computer System Evaluation Criteria (TCSEC).

(02 mark)

ANSWER IN THIS BOX

2) (a) Which mode of operation of the Advanced Encryption Standard (AES) block cipher would you use to protect electronic fund transfer? Give a brief justification for your answer.

(05 mark)

ANSWER IN THIS BOX

(b) List two (2) block cipher encryption modes that can produce a stream cipher.

(04 mark)

ANSWER IN THIS BOX

(c) Describe two (2) problems associated with the symmetric key encryption method.

(06 mark)

ANSWER IN THIS BOX

(d) Nimal has a RSA public key (n, e) = (33, 3) and a private key = (n, d) = (33, 7). Suppose Nimal generates the plain text M=2 to be digitally signed. Determine the digital signature S of M.

(05 mark)

ANSWER IN THIS BOX

3) (a) Describe "two factor authentication" mechanism by using an example.

(05 mark)

ANSWER IN THIS BOX

(b) "Given the number of employees, the mean salary for a company and the mean salary of all employees except the Director, it is easy to compute the Director's salary." Briefly discuss the implications of above statement with regard to database security.

(05 mark)

ANSWER IN THIS BOX

(c) List any five (5) key security features of a trusted operating system.

(05 mark)

ANSWER IN THIS BOX

(d) What are the necessary steps that should be taken in order to avoid a disaster with regard to a critical information system such as a Core Banking System?

(05 mark)

ANSWER IN THIS BOX

4) (a) List three(3) ISO security services supported by Secure Shell (SSH) protocol.

(03 marks)

ANSWER IN THIS BOX

(b) Explain the security gateway to security gateway network configuration scenario that is used by the IPSec protocol use a simple diagram.

(06 marks)

ANSWER IN THIS BOX

(c) List five (5) best practices with regard to e-mail security.

(05 marks)

ANSWER IN THIS BOX

(d) Explain the operation of the **Secure Socket Layer (SSL) Record** protocol.

(06 marks)

ANSWER IN THIS BOX

****