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:					

Index No: ……...

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

False

Justification: According to Shannon, the size of enciphered text should be no larger than the text of the original message.

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

(02 marks)

ANSWER IN THIS BOX

False

Justification: The Vernam Cipher is an example of a Stream cipher. A block cipher encrypts a group of plaintext symbols as one block.

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

(02 marks)

ANSWER IN THIS BOX

True

Justification: The AES algorithm as defined can use 128, 192 or 256 bit keys.

(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

False

Justification: A symmetric key system with n users requires n * (n - 1)/2 keys. Thus 10 users require 10*(10-1)/2=45 keys.

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

(02 marks)

ANSWER IN THIS BOX

True

Justification: The Euclidean algorithm exploits the fact that if x divides a and b, x also divides a - (k * b) for every k. Thus it can be used to compute the greatest common divisor of two numbers.

(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

False

Justification: A Network-based Intruder Detection System (NIDS) is a stand-alone device attached to the network to monitor traffic throughout that network; a host-based IDS runs on a single workstation or client or host to protect that one host.

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

(02 marks)

ANSWER IN THIS BOX

False

Justification: PGP depends on each user exchanging keys with all potential recipients and establishing a ring of trusted recipients.

(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

Fasle

Justification: Non-repudiation means that customers or partners can be held accountable for transactions, such as online purchases, which they cannot later deny.

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

(02 marks)

ANSWER IN THIS BOX

True

Justification: A firewall filters incoming and outgoing network traffic thus keeping certain. kinds of network traffic out of a private network.

(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

True

Justification: Hackers use dictionaries to find password. Thus organizations also can use dictionaries to guard a password against easy-to-guess passwords.

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

(02 marks)

ANSWER IN THIS BOX

True

Justification: Symmetric algorithms have key distribution problem but asymmetric algorithms do not have this problem. In contrast to that, asymmetric algorithms are slower than symmetric algorithms. Thus popular cryptographic protocols use a hybrid combination of symmetric and asymmetric algorithms.

(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

False

Justification: A logic bomb executes when a specified condition occurs. Zombie is a class of malicious code that executes various commands sent by a remote attacker.

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

(02 marks)

ANSWER IN THIS BOX

True

Justification:

123309 = 13 x 9315 + 2214	gcd(9315, 2214
9315 = 4 x 2214 + 459	gcd(2214,459)
2214 = 4 x 459 +378	gcd(459,378)
459 = 1 x 378 +81	gcd(378,81)
378 = 4 x 81 + 54	gcd(81,54)
81 = 1 x 54 +27	gcd(54,27)
54=2*27+0	

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

(02 mark)

ANSWER IN THIS BOX

False

Justification: Copyright protects the expression of an idea and a patent protects the invention.

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

(02 mark)

ANSWER IN THIS BOX

True

Justification: They do not have common factors.

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

(02 mark)

ANSWER IN THIS BOX

False

Justification: The Digital Signature Algorithm (DSA) can be used only for signing but RSA can be used for signing and encryption.

(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

True

Justification:

For the private key x and public key X, we have the relation $X = g^x \pmod n$.

public key of A (X) = $3^5 \pmod{10}$; X= 243 (mod 10), X=3
Thus session key (k) =$X^y \pmod{n.}$ =$3^6 \pmod{10}$ = 9

(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

False

Justification: Kerberos authentication protocol requires two systems, called the Authentication Server (AS) and the Ticket-Granting Server (TGS), which are both part of the Key Distribution Center (KDC).

(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

False

Justification: Mandatory Access Control (MAC) means that access control policy decisions are made beyond the control of the individual owner of an object. By contrast, Discretionary Access Control (DAC) leaves a certain amount of access control to the discretion of the object's owner or to anyone else who is authorized to control the object's access.

(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

True

Justification: The Bell and La Padula model is a formal description of the allowable paths of information flow in a secure system. The model has been used to define security requirements for systems concurrently handling data at different sensitivity levels.

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

Cipher Block Chaining (CBC) mode is suitable for electronic fund transfer since it can provide data integrity and data confidentiality security services.

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

(04 mark)

ANSWER IN THIS BOX

1. Cipher Feedback Mode (CFB) mode
2. Output Feedback (OFB) mode

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

(06 mark)

ANSWER IN THIS BOX

Student should briefly describe the following two problems.

01 Key distribution problem

02 Key management problem

(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

Signing

$S=M^d \pmod n$

M=2, d=7 and n=33, so that $S= 2^7 \pmod{33}$*; S=29*

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

(05 mark)

ANSWER IN THIS BOX

A two factor authentication mechanism combines two authentication mechanisms that list under the following authentication principles.

1. Something the user knows
2. Something the user has
3. Something the user is

Automatic Teller Machine (ATM) card is the best example for two factor authentication. It uses a plastic card with the magnetic script (Something the user has) and Personal Identification Number (PIN) (Something the user knows) for authentication of a banking user.

(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

Students should explain the data inference problem. For example:

Statement Avg(A1,A2,A3) and Avg(A1,A2), inferences the value of A3

A3. A1, A2 and A3 are data fields of a database.

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

(05 mark)

ANSWER IN THIS BOX

Any five(5) from the following list:

1. user identification and authentication
2. mandatory access control
3. discretionary access control
4. object reuse protection
5. trusted path
6. audit logs
7. intrusion detection

(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

- Maintain backups securely at off-site
- Deploy twin sites for computer equipment
- Insure the system with a disaster recovery firm
- Establish a disaster recovery plan
- Periodically test the disaster recovery plan

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

(03 marks)

ANSWER IN THIS BOX

Authentication

Integrity

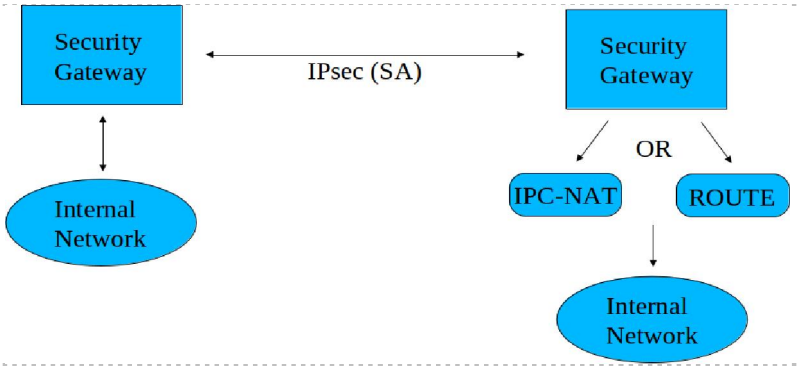
Confidentiality

(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

Student should explain the following diagram.



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

(05 marks)

ANSWER IN THIS BOX

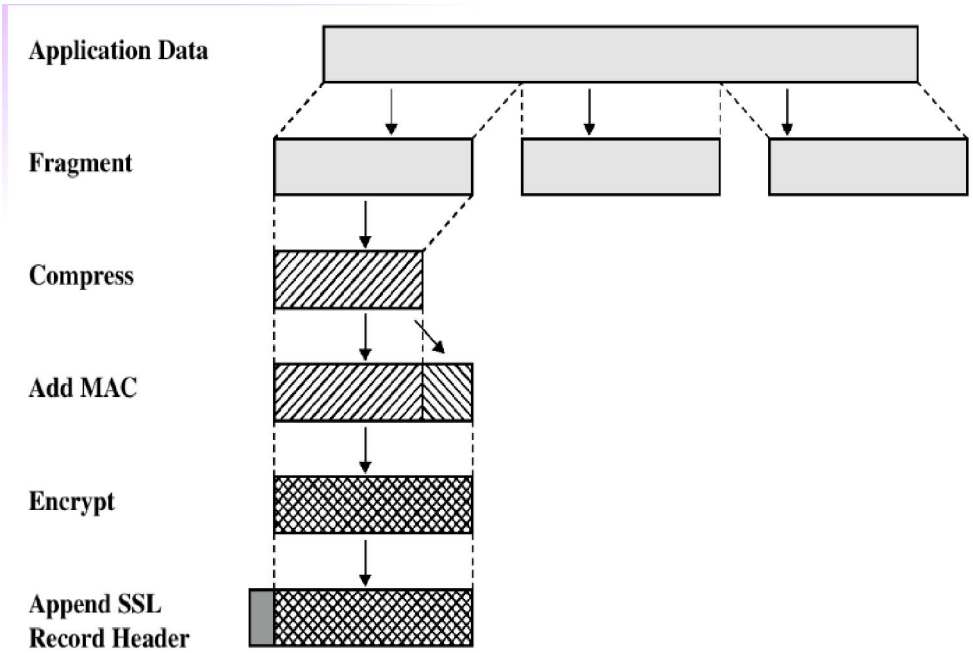
1. Use the BCC field when sending e-mails to large distribution lists to protect recipient email addresses.
2. Beware of reply to all button while replying an e-mail.
3. Avoid use of large distribution lists unless it is a legitimate business purpose.
4. Do not forward chain email letters.
5. Use PGP or S/MIME security services to provide authentication, integrity and confidentiality of an e-mail

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

(06 **marks)**

ANSWER IN THIS BOX

Student should explain the following digram.



****