UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2012/2013 – 3rd Year Examination – Semester 5

IT5204: Information Systems Security

Structured Question Paper

16th March, 2013

(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) State whether each of the following statements are **true** or **false**, and then briefly justify giving reasons for your answer.

(a) The cipher text **C = Khoor Gu Ndvxq** will be decrypted to the plain text **P = Hello Mr Kamal** by the Cesar cipher.

(02 marks)

ANSWER IN THIS BOX

False

Justification:

Cipher text C= Khoor Gu Ndvxq is equal to the plain text P = Hello Dr Kasun as Cesar Cipher: C(i)=P(i)+3

(b) The Data Encryption Standard (DES) is an example of a stream cipher.

(02 marks)

ANSWER IN THIS BOX

False

Justification: A block cipher encrypts a group of plaintext symbols as one block, hence DES is an example of a Block cipher.

(c) The Advanced Encryption Standard (AES) algorithm uses 64 bit data blocks.

(02 marks)

ANSWER IN THIS BOX

False

Justification: The AES algorithm uses 128 bit data blocks.

(d) A symmetric key system with five (5) users requires 10 keys and each user must track and remember a key for each other user with whom he or she wants to communicate.

(02 marks)

ANSWER IN THIS BOX

Ture

Justification: 5 users require 5*(5-1)/2=10 keys as a symmetric key system with n users requires n * (n - 1)/2 keys.

(e) The Secure Hash Algorithm (SHA) can be used to implement an authentication protocol.

(02 marks)

ANSWER IN THIS BOX

True

Justification: An authentication protocol keeps the hash of a user password to implement SHA.

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

(02 marks)

ANSWER IN THIS BOX

True

Justification: NIDS is a stand-alone device attached to the network to monitor traffic throughout that network as a host-based IDS runs on a single workstation or client or host to protect that one host.

(g) The SSL protocol is an example of a hybrid encryption protocol.

(02 marks)

ANSWER IN THIS BOX

True

Justification: One of the most important advantages of the SSL protocol is mixing the better of two encryption key techniques symmetric and asymmetric.

(h) The concept of authentication means that customers or partners can be held accountable for transactions, such as online purchases, which they cannot later deny after being made.

(02 marks)

ANSWER IN THIS BOX

False

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 honeypot is a device that keeps certain kinds of network traffic out of a private network.

(02 marks)

ANSWER IN THIS BOX

False

Justification: A honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.

(j) A fingerprint based attendance system provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX

True

Justification: In the fingerprint based attendance system, a user needs to enters the PIN and put the finger so it provides two factor authentication.

(k) A computer virus is a unpublished and undocumented entry point into a computer program.

(02 marks)

ANSWER IN THIS BOX

False

Justification:

A computer virus is a malicious computer program that can copy itself and infect a computer without the permission or knowledge of the owner and a trapdoor is a secret undocumented entry point into a computer program.

(l) Risk analysis is a well-known planning tool used often by auditors, accountants and information security managers.

(02 marks)

ANSWER IN THIS BOX

True

Justification: In many situations, such as obtaining approval for a new security system, a risk analysis is required. Risk analysis tools are used in preparation for creating a security plan.

(m) The greatest common divisor of 345 and 436 is 3.

(02 marks)

ANSWER IN THIS BOX

True

Justification:

GCD(345,456) → GCD(456,345) → GCD(345,111) → GCD(111,12) → GCD(12,3) → GCD = 3 → **gcd(345,436) =3**

(n) A trade secret can protect against a pirate who sells copies of someone else's program without permission.

(02 marks)

ANSWER IN THIS BOX

False

Justification: Trade secret cannot protect against a pirate who sells copies of someone else's program without permission. However, trade secret protection makes it illegal to steal a secret algorithm and use it in another progrram.

(o) (18, 9), (8,2), (16,4) are relatively prime numbers.

(02 marks)

ANSWER IN THIS BOX

False

Justification: Relatively prime numbers should not have common factors.

(p) The RSA algorithm can be used for signing and encryption.

(02 marks)

ANSWER IN THIS BOX

True

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

(q) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points, A and B, and we have chosen the integer 5 as g and the integer 11 as n. If A generates the private key x=2 and B generates the private key y=3, the session key k between A and B is 9.

(02 marks)

ANSWER IN THIS BOX

False

Justification:

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

public key of A (X) = 5^2 mod 11; X= 25 mod 11,   X=3

Thus session key (k) =g^y mod n. =5^3 mod 11 = 625 mod 11 =5

(r) Anonymity preserves privacy in the Internet.

(02 marks)

ANSWER IN THIS BOX

True

Justification: One way to preserve privacy is to guard our identity. Not every context requires us to reveal our identity, so some people use anonymity to protect privacy.

(s) In Kerberos authentication protocol, an Authentication Server (AS) issues a login ticket to the Kerberos client.

(02 marks)

ANSWER IN THIS BOX

False

Justification: In Kerberos authentication protocol, a Ticket-Granting Server (TGS) issues a login ticket to the Kerberos client.

(t) Mandatory Access Control (MAC) 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.

(02 marks)

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.

2) (a) List the five (5) Shannon characteristics that identify a good cipher.

(05 Marks)

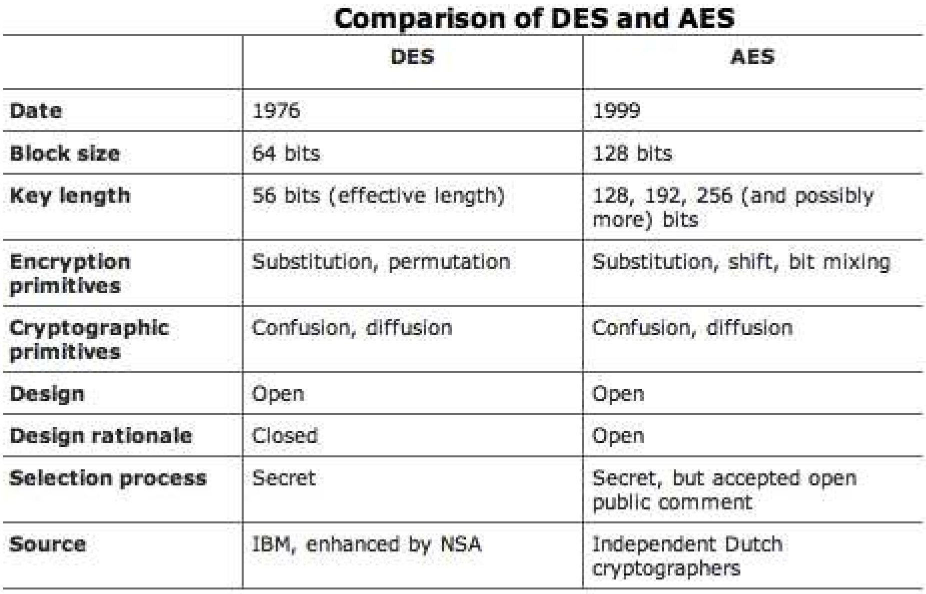
ANSWER IN THIS BOX

1. The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
2. The set of keys and the enciphering algorithm should be free from complexity.
3. The implementation of the process should be as simple as possible.
4. Errors in ciphering should not propagate and cause corruption of further information in the message.
5. The size of the enciphered text should be no larger than the text of the original message.

(b) Compare five (5) characteristics of Data Encryption Standard (DES) and Advanced Encryption Standard (AES).

(05 Marks)

ANSWER IN THIS BOX



Comparison of DES and AES

	DES	AES
Date	1976	1999
Block size	64 bits	128 bits
Key length	56 bits (effective length)	128, 192, 256 (and possibly more) bits
Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accepted open public comment
Source	IBM, enhanced by NSA	Independent Dutch cryptographers

(c) Which mode of operation of the Advanced Encryption Standard (AES) block cipher would one use to protect a live video stream? Give a brief justification for your answer.

(05 Marks)

ANSWER IN THIS BOX

Stream ciphers are suitable for real-time encryption. Cipher Feedback Mode or Output Feedback Mode converts a block cipher into a stream cipher. Thus these two modes are suitable to encrypt a live video stream.

(d) Consider the following scenario.

Nimal has RSA public key (n, e) = (33, 3) and private key = (n, d) = (33, 7). Kamala has RSA public key (n, e) = (55, 7) and private key = (n, d) = (55, 23). Suppose Nimal generates the plain text M=2 to be encrypted and send to Kamal. Determine the cipher text C.

(05 Marks)

ANSWER IN THIS BOX

Encryption

$C=M^e$ mod n

$M=2$, $e=7$ and $n=55$, so that 2^7 mod 55; $C=18$

3) (a) In a given situation, a password consist of uppercase characters an English Alphabet and is of variable length from 1 to 5 characters. How may days would it take to determine a particular password, assuming that testing an individual password requires 2 second and a brute force technique is used?

(05 Marks)

ANSWER IN THIS BOX

If passwords are words consisting of the 26 characters A .. Z and can be of any length from 1 to 5 characters, there are 26^1 passwords of 1 character, 26^2 passwords of 2 characters, and 26^5 passwords of 5 characters.

Therefore, the system as a whole has $26^1 + 26^2 + 26^3 + 26^4 + 26^5 = 12356630$ passwords. If we were to use a computer to create and try each password at a rate of checking one password per 2 second, it would take on the order of 1256630*2/(60*60*24) ~ 286 days to test all passwords.

(b) Draw an access control matrix to represent the following conditions.

1. Subjects are U1, U2, U3 and U4
2. Objects are File1, File2, Program1 and Program2
3. U1 can read File1 and execute Program2
4. U2 can read File2
5. U3 can execute Program1 and Program2
6. U4 can read and write all objects

(05 Marks)

ANSWER IN THIS BOX

	File1	File2	Program1	Program2
U1	R			X
U2		R		
U3			X	X
U4	R,W	R,W	R,W	R,W

R -Read; W- Write; X- Execute

(c) List five (5) memory protection methods that can be used to prevent one program from affecting the data and programs in the memory space of other users.

(05 Marks)

ANSWER IN THIS BOX

1. Fence
2. Relocation
3. Base/bounds register
4. Segmentation
5. Paging

(d) Briefly describe the role of an Attribute Authority (AA).

(05 Marks)

ANSWER IN THIS BOX

An authority trusted by one or more users to create and sign attribute certificate. It is important to note that the AA is responsible for the attribute certificates during their whole lifetime, not just for issuing them.

4) (a) List four (4) ISO security services supported by the S/MIME standard.

(04 Marks)

ANSWER IN THIS BOX

Authentication

Integrity

Confidentiality

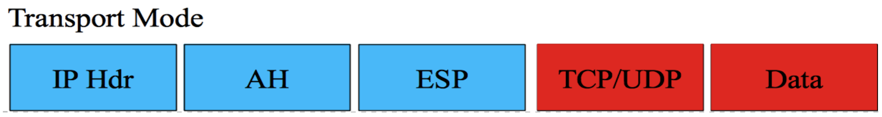
non-repudiation

(b) Suppose one wants to authenticate and encrypt the IP packets (excluding the IP address) by using IPSec protocol. Explain the structure of a IPSec packet by using a suitable diagram.

(06 Marks)

ANSWER IN THIS BOX

Student explain the following digram.

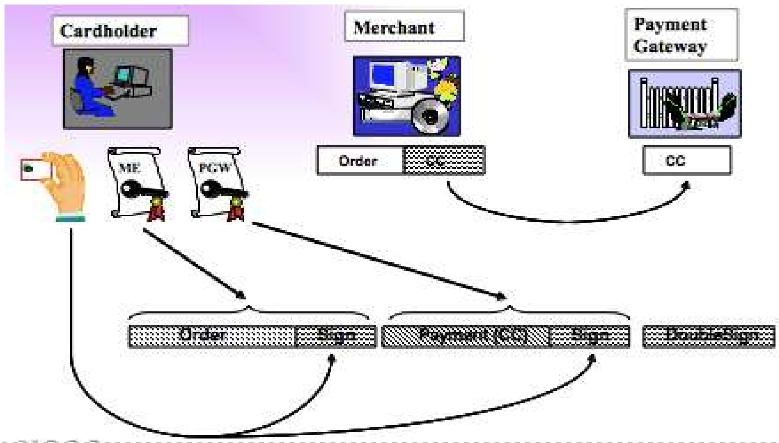


(c) Using a suitable diagram, briefly explain the structure of the Payment Request Message of the Secure Electronic Transaction (SET) protocol.

(05 Marks)

<u>ANSWER IN THIS BOX</u>

Student should explain the following diagram.



(d) “Humans are said to be the weakest link in any security system”. Express your views on the above statement by using a simple example.

(05 Marks)

<u>ANSWER IN THIS BOX</u>

Student should take an example such as “write down password on papers” and explain the problem.

******