Index No: ……...

UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)
Academic Year 2017 – 3rd Year Examination – Semester 5

IT5205: Information Systems Security

Structured Question Paper

03 June, 2017

(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 **15 pages**.
- **Answer all 4 questions**. (all questions **do not** carry equal marks)
- **Question 1 and 2 (**30% marks each**) 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. [×]) 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) If p is a prime number, for any number q<p, greatest common divisor is equal to 1 (gcd(p,q)=1).

(02 marks)

ANSWER IN THIS BOX
TRUE
A number that cannot be factored further is called a prime number.
Thus any number q which is less than p should not have common facters.

(b) The security of the encryption scheme must depend only on the secrecy of the algorithm.

(02 marks)

ANSWER IN THIS BOX
False
The security of the encryption scheme must depend only on the secrecy of the key
and not on the secrecy of the algorithm.

(c) The Data Encryption Standard (DES) algorithm encrypts **sixteen (16)** bytes of a plain text message to the **sixteen (16)** bytes of a cipher text message when DES uses Electronic Code Book (ECB) mode and Public Key Cryptography Standard 5 (PKCS5) padding scheme.

(02 marks)

ANSWER IN THIS BOX
False
PKCS5 padding inserts new dummy block when the plain text size equals to the block
size of the cipher algorithm. The block size of DES algorithm is 8 bytes.
Hence cipher text size will be 24 bytes when the plain text size equals to 16 bytes.

(d) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two end points, A and B, and we have chosen the integer **g=3** and the integer **n=10**. If A generates the private key **x=3** and B generates the private key **y=2**, the session key **k** between A and B is **9**.

(02 marks)

ANSWER IN THIS BOX
True
For the private key x and public key X, we have the relation $X = g^x \bmod n$.
public key of A (X) = $3^3 \bmod 10$; X= 27 mod 10, X=7
public key of B (Y) = $3^2 \bmod 10$; Y= 9 mod 10, Y=9
Session key k = $X^y \bmod n$: k=$7^2 \bmod 10$ k= 9 OR
Session key k = $Y^x \bmod n$: k=$9^3 \bmod 10$ k= 9

(e) Nimal has RSA public key **(n, e) = (33, 3)** and private key = **(n, d) = (33, 7)**. Suppose Nimal sings plain text message **M=3** to Kamal. Kamal receives signature (S)=**8**.

(02 marks)

ANSWER IN THIS BOX
False
$S=P^d \bmod n$
$S=3^7 \bmod 33=2187 \bmod 33=9$

(f) Precautions against unauthorized modification falls in to the category of data confidentiality.

(02 marks)

ANSWER IN THIS BOX
False
Detecting an unauthorized modification is called data integrity.

(g) The MD5 hash algorithm generates **128** bit hash value when the input message length equals to **eight (8)** bytes and generates **160** bit hash value when the input message length equals to **sixteen (16)** bytes.

(02 marks)

ANSWER IN THIS BOX
False
The hash size only depends on the algorithm.
It does not depend on the length of the input message.
The MD5 always generates 128 bit hash values irrespective of the message length.

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

(02 marks)

ANSWER IN THIS BOX
True
One of the most important advantages of the SSL protocol is mixing
the better of two encryption key techniques symmetric and asymmetric.
Therefore it is an example of a hybrid protocol.

(i) One of the ISO security service supports by the **PGP** standard is **non-repudiation**.

(02 marks)

ANSWER IN THIS BOX
True
ISO security services supported by the PGP standard are:
authenticity, integrity confidentiality and non-repudiation.

(j) An ATM cards provides three-factor authentication.

(02 marks)

ANSWER IN THIS BOX
False
An ATM cards, a user needs to enters the PIN and put the finger.
Thus it provides two factor authentication.

(k) Risk analysis is a well-known planning tool, used by information security managers to organize a security training programs.

(02 marks)

ANSWER IN THIS BOX
False
In many situations, such as obtaining approval for new security system,
a risk analysis is required.
Risk analysis tools use in preparation for creating a security plan
not for planing a security training programs.

(l) In Kerberos authentication protocol, a Ticket-Granting Server (TGS) issues a ticket granting ticket to the Kerberos client.

(02 marks)

ANSWER IN THIS BOX
False
In Kerberos authentication protocol, an Authentication Server (AS) issues
a ticket granting ticket to the Kerberos client.
Ticket-Granting Server (TGS) issues a login ticket to the Kerberos client.

(m) If passwords are words consisting of the 26 characters A .. Z and can be of any length from 1 to 5 characters, 5^{26} passwords are available to use.

(02 marks)

ANSWER IN THIS BOX
False
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.

(n) A threat is a weakness in the security system that might be exploited to cause loss or harm.

(02 marks)

ANSWER IN THIS BOX
False
A vulnerability is a weakness in the security system
that might be exploited to cause loss or harm.
A threat to a computing system is a set of circumstances
that has the potential to cause loss or harm.

(o) Hardware Security Module (HSM) provides more timely information regarding the revocation status of a certificate.

(02 marks)

ANSWER IN THIS BOX
False
Online Certificate Status Protocol (OCSP) provides more timely information
regarding the revocation status of a certificate.

2) **Select the correct answer, and then say why in at most one sentence.**

a) What common attack can be used against passwords if a copy of the password file can be obtained?

a) Birthday attack

b) Dictionary attack

c) Plaintext attack

d) Smurf attack

(02 marks)

ANSWER IN THIS BOX
(B)- Correct - Encrypting each word in a dictionary of commonly used words
or known password styles and seeing if the hashed value is the same
as the hash value stored in the password file.

b) What is the **first** step to be performed in establishing a **Disaster Recovery Plan**?

a) Demonstrate adherence to a standard disaster recovery process

b) Agree on the goals and objectives of the plan

c) Identify applications to be run during a disaster

d) Determine the site to be used during a disaster

(02 marks)

ANSWER IN THIS BOX
(B)-Correct - Agree on the goals and objectives of the plan is a
critical component of disaster recovery plan.

c) Which device can be used to segment and protect networks from each other?

a) Network switch

b) Firewall

c) Proxy server

d) Segmentation server

(02 marks)

ANSWER IN THIS BOX
(B)- Correct- The primary objective of a firewall is the protection
of those assets that reside behind it.

d) A computer virus most frequently spreads via

a) User misuse

b) Exploitation of vulnerabilities in software

c) Mobile code attacks

d) Infected USB drives and e-mails

(02 marks)

ANSWER IN THIS BOX
(D) - Correct – A virus usually spreads as e-mail attachments and infected USBs.

e) An encrypted communications tunnel created between two systems, and used for secure communications, is called a;

a) Leased Line

b) Chinese Firewall

c) Named-pipe

d) Virtual Private Network (VPN)

(02 marks)

ANSWER IN THIS BOX
(D)-Correct- By definition, a VPN provides a secure tunnel from one site
to another over an insecure environment such as the Internet.

f) Which one of the following can be used to increase the authentication strength of an access control system?

a) Multi-party

b) Two Factor

c) Mandatory

d) Discretionary

(02 marks)

ANSWER IN THIS BOX
(B) – Correct - Using two of the three factors (something you know,
something you have, and something you are) increase the strength of authentication.

g) Which trusted third party authenticates public encryption keys?

a) Public Key Notary

b) Certification Authority

c) Key Distribution Center

d) Key revocation certificate

(02 marks)

ANSWER IN THIS BOX
(B) - Correct – a Certification Authority authenticates Public Keys.

h) Which of the following defines the intent of a system security policy?

a) A description of the settings that will provide the highest level of security

b) A brief, high-level statement defining what is and is not permitted in the operation of the system

c) A definition of those items that must be denied on the system

d) A listing of tools and applications that will be used to protect the system

(02 marks)

ANSWER IN THIS BOX
(B) - Correct - Policy is a high-level document outlining management priorities,
objectives, compliance, discipline, and user behaviors.

i) An advantage of asymmetric key cryptography is that

a) It is relatively easy to distribute keys

b) Both keys are the same

c) It can be easily implemented in hardware

d) Its execution is very fast

(02 marks)

ANSWER IN THIS BOX
(A) - Correct - one of the greatest uses of asymmetric key cryptography is
to negotiate or distribute symmetric keys and the ease of distributing the public keys of the users.

j) What are the three objectives of information security?

a) Prevent, detect, respond

b) Integrity, authenticity, and completeness

c) Confidentiality, integrity, and availability

d) Identification, authentication, non-repudiation

(02 marks)

ANSWER IN THIS BOX
(C) Correct – CIA is the standard definition of Information Security

k) Which of the following technologies would best secure the data on a laptop or other device that could be stolen?

a) Data encryption

b) File deletion

c) No access to the floppy drive

d) Steganography

(02 marks)

ANSWER IN THIS BOX
(A) - Correct – Full Disk Encryption is the best method that can be used to secure the data on a laptop

l) Which type of malicious detection software would detect a polymorphic virus by comparing the function of the application rather than comparing it to a known signature?

a) Host-based intrusion detection

b) Network-based intrusion detection

c) Gateway anti-virus scanner

d) Heuristic scanner

(02 marks)

ANSWER IN THIS BOX
(D) Correct – Heuristic analysis determines changes to expected
behaviour of an application or system.

m) Which of the following does a digital signature provide?

a) It gives you the ability to encrypt an individual's confidential data

b) It ensures a individual's privacy

c) It identifies the source and verifies the integrity of data

d) It provides a framework for law and procedures

(02 marks)

ANSWER IN THIS BOX
(C) - CORRECT- Digital signatures confirm the source and can assure the integrity of the data.

n) Security of an automated information system is most effective and economical if the system is

a) Initially optimized and security controls applied to it

b) Customized to meet the specific security threat

c) Subjected to intense security testing after implementation

d) Created from a design that has the necessary, appropriate, and proportional controls built-in

(02 marks)

ANSWER IN THIS BOX
(D)- Correct - The keywords here are "effective AND economical".
The later you find a problem, the more it costs to fix it.

o) Which best describes a **qualitative** risk analysis?

a) A probabilistic method for risk assessment

b) A method used to apply severity levels to potential loss, probability of loss, and risks

c) A method that assigns monetary values to components in the risk assessment

d) A method that is based uses opinions of individuals and a rating system to gauge the severity level of different threats and the benefits of specific countermeasures.

(02 marks)

ANSWER IN THIS BOX
(D) - Correct - A qualitative analysis uses opinions of individuals and
a rating system to gauge the severity level of different threats and
the benefits of specific countermeasures.

3) (a) What is the trusted registry that guarantees the authenticity of client and server public keys?

(05 marks)

ANSWER IN THIS BOX
Certification Authority (CA)

(b) State the concepts of **Authentication**, **Authorization** and **Accountability** with respect to information systems.

(06 marks)

ANSWER IN THIS BOX
Authentication is the process of determining whether someone or something is,
in fact, who or what it is declared to be.
Authorization is the function of specifying access rights to resources,
which is related to information security.
Accountability refers to the record-keeping and tracking of user
activities on a computer network.

(c) Define the terms **Unconditional Secure** and **Computational Secure** with respect to the cryptographic algorithms.

(04 marks)

ANSWER IN THIS BOX
Unconditional secure essentially means security against an adversary
with unbounded computational power.
Cryptographic algorithm is **computationally** secure
when a computer is unable to decipher a code within a certain amount of time.

(d) What is phishing scam?

(05 marks)

ANSWER IN THIS BOX
Phishing scams are attempts by scammers to trick you into giving out personal
information such as your bank account numbers, passwords and credit card numbers.

4) a) IPSec is a framework for securing IP packets sent through the public Internet. Depending on the amount of security we need, it is possible to configure IPSec in different ways. IPSec ESP (Encapsulating Security Payload) Tunnel Mode is such a configuration. Using a suitable diagram,explain how IPSec ESP Tunnel Mode works to protect an IP datagram with a TCP payload.

(07 marks)

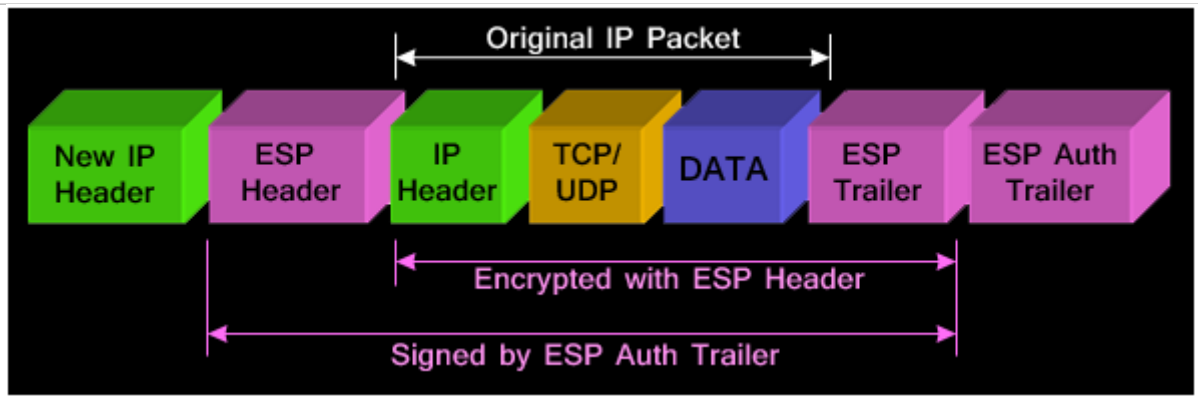
ANSWER IN THIS BOX

Tunnel mode is used to encrypt traffic between secure IPSec Gateways,

In tunnel mode, an IPSec header (AH or ESP header) is inserted between

the IP header and the upper layer protocol.

The packet diagram below illustrates IPSec Tunnel mode with ESP header:



b) Briefly explain the TLS authentication process.

(06 marks)

ANSWER IN THIS BOX

For server authentication, the client uses the server's public key to encrypt
the data that is used to compute the secret key. The server can generate the secret key
only if it can decrypt that data with the correct private key.

For client authentication, the server uses the public key in the client certificate to decrypt
the data the client sends during the handshake. The exchange of finished messages that
are encrypted with the secret key confirms that authentication is complete.

If any of the authentication steps fail, the handshake fails and the session terminates.
The digital certificates are exchanged during the TLS handshake.

c) Technical, Administrative, and Physical is one way of categorising Information Security Controls. Describe another way of categorising security controls depending on the action performed by the control.

(07 marks)

ANSWER IN THIS BOX
Deterrent: Intended to discourage a potential attacker
Preventive: Intended to avoid an incident from occurring
Corrective: Fixes components or systems after an incident has occurred (Reactive)
Recovery: Intended to bring controls back to regular operations
Detective: Helps identify an incident's activities
Compensating: Controls that provide for an alternative measure of control
Directive: Mandatory controls that have been put in place due to regulations or environmental requirements

****