Index No: ……..

UNIVERSITY OF COLOMBO, SRI LANKA

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2020 – 3rd Year Examination – Semester 5

IT5205: Information Systems Security

Structured Question Paper

(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** on **15 pages**.
- **Answer all 4 questions**. (all questions **do not** carry equal marks)
- **Question 1 and 2** carry 30 marks each **and other two 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:					

1) **State whether each of the following statements is true or false, and then briefly justify your answer.**

(a) Suppose users in two offices would like to access each other's file servers over the Internet. Virtual private network (VPN) security control could only provide authenticity for such communication.

(02 marks)

ANSWER IN THIS BOX
False
Virtual private network (VPN) security control would provide
confidentiality for those communications.

(b) Suppose we have nodes A, B, C, D and E in a network. We have to generate a total of nine (9) keys to let every node communicate with every other node in a bidirectional secure way using the AES encryption algorithm.

(02 marks)

ANSWER IN THIS BOX
False
Number of keys = number of node * (number of nodes - 1)/2
Number of keys = 5*4/2=10

(c) The Advanced Encryption Standard (AES) algorithm encrypts **fifty four (54)** bytes of a plain text message to **sixty four (64)** bytes of a cipher text message when it uses Electronic Code Book (ECB) mode and the Public Key Cryptography Standard 5 (PKCS5) padding scheme.

(02 marks)

ANSWER IN THIS BOX
True
The block size of AES algorithm is 16 bytes.
Hence cipher text size will be 64 bytes when the plain text size equals to 54 bytes.

(d) Suppose we want to use the Diffie-Hellman Key Agreement protocol between two parties, A and B, and we have chosen the integer **g=5** and the integer **n=11**. 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 **7**.

(02 marks)

ANSWER IN THIS BOX
False
For the private key x and public key X, we have the relation $X = g^x \bmod n$.
public key of A (X) = $5^3 \bmod 11$; X= 125 mod 11, X=4
public key of B (Y) = $5^2 \bmod 11$; Y= 25 mod 11, Y=3
Session key k = $X^y \bmod n$: k=$4^2 \bmod 11$, 16 mod 11 k= 5 OR
Session key k = $Y^x \bmod n$: k=$3^3 \bmod 11$, 27 mod 11 k= 5

(e) Nimal has RSA public key **(n, e) = (33, 3)** and private key = **(n, d) = (33, 7)**. Kamal has RSA public key **(n, e) = (91, 11)** and private key = **(n, d) = (91, 59)**. Suppose Nimal encrypts plain text message **M=2** to Kamal. Kamal receives cipher text message **C = 27**.

(02 marks)

ANSWER IN THIS BOX
False
$C=P^e \bmod n$
$C=3^{11} \bmod 91=2048 \bmod 91=46$

(f) Nimal has RSA public key **(n, e) = (33, 3)** and private key = **(n, d) = (33, 7)**. Kamal has RSA public key **(n, e) = (91, 11)** and private key = **(n, d) = (91, 59)**. Suppose Nimal signs a plain text message **M=2**. Nimal's signature will be S = **9**.

(02 marks)

ANSWER IN THIS BOX
False
$C=P^d \bmod n$
$C=2^7 \bmod 33=128 \bmod 33=29$

(g) The SHA-256 hash algorithm generates a **32** bit hash from an input message of **sixty four (64)** bits.

(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 SHA-256 always generates 256 bit hash values
irrespective of the message length.

(h) The **Transport Layer Security (TLS)** protocol is an example of a hybrid encryption standard.

(02 marks)

ANSWER IN THIS BOX
True
TLS uses
two categories of the cryptographic algorithms symmetric and asymmetric.
Therefore it is an example of a hybrid standard.

(i) One of the ISO security services supported by the **S/MIME standard** is **non-repudiation**.

(02 marks)

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

(j) Vendors publish MD5 hash values when they provide software patches for their customers in order to verify software integrity.

(02 marks)

ANSWER IN THIS BOX
True
A Hashing algorithm provides the software integrity. Thus vendors publish MD5 hash values when they provide software patches.

(k) If p is a prime number, for any number q<p, greatest common divisor of p and q is equal to q that is gcd(p,q)=q.

(02 marks)

ANSWER IN THIS BOX
False
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 factors other than 1.

(l) A bank ATM card provides two-factor authentication.

(02 marks)

ANSWER IN THIS BOX
True
In using a ATM card, a user needs to insert the card and enter the PIN.
Thus it provides two factor authentication.

(m) The domain of security **Controls** may be categorised into **Physical**, **Technical**, and **Administrative** controls. A **Security Policy** is an example of **Administrative** control.

(02 marks)

ANSWER IN THIS BOX
True
Technical Controls involves the use of safeguards incorporated in applications
software and related devices.
Administrative Controls consists of management constraints,
operational procedures and accountability procedures.
Thus Security Policy is an example of administrative Control.

(n) Kasun recently implemented an intrusion prevention system designed to block common network attacks from affecting his organization. This is an example of **Risk Mitigation**.

(02 marks)

ANSWER IN THIS BOX
True
Risk mitigation strategies attempt to lower the probability and/or impact of a risk occurring.
Intrusion prevention systems attempt to reduce the probability of a successful attack
and are, therefore, examples of risk mitigation.

(o) The Vernam cipher encrypts plain text P = 1011 0110 1011 to the cipher text C = 0101 1100 0100 with the security key K= 1110 1010 1111.

(02 marks)

ANSWER IN THIS BOX	
True	
Plain Text	= 1011 0110 1011
Key	= 1110 1010 1111
Cipher Text	= 0101 1100 0100

2) **For each of the questions, select the correct answer, and then say why it is correct, <u>in at most one sentence</u>.**

a) Which of the following is not an example of physical data leakage?

i. Phishing
ii. Dumpster diving
iii. Shoulder surfing
iv. Printers and photocopiers

(02 marks)

ANSWER IN THIS BOX
(i) CORRECT: Phishing is the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in an electronic communication.

b) When a person is harassed repeatedly by being followed the person is called a target of

i. Bullying
ii. Stalking
iii. Identity theft
iv. Phishing

(02 marks)

ANSWER IN THIS BOX
(ii) CORRECT: Stalking is unwanted or repeated surveillance.

c) Which one of the following modes of operation in AES is used for operating short length data?

i. Cipher Feedback Mode (CFB)
ii. Cipher Block chaining (CBC)
iii. Electronic code book (ECB)
iv. Output Feedback Modes (OFB)

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: In ECB mode, repetitions in Plain Text lead to repetitions in Cipher Text. Thus it is used for operating only on short data.

d) Which of the following security tools deals with network intrusion detection and real-time traffic analysis?

i. John the Ripper
ii. L0phtCrack
iii. Snort
iv. Nessus

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: Snort helps in matching patterns against known attack patterns and protect your network.

e) Which of the following is not a protocol that uses cryptography?

i. SSH
ii. SSL
iii. SMTP
iv. SFTP

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: SMTP (Simple Mail Transfer Protocol) is a standard protocol to transmit
electronic mail and is a widely used mail transmitting protocol.

f) Which of the following is **not** a threat to information security?

i. Disaster
ii. Eavesdropping
iii. Unchanged default password
iv. Information leakage

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: Disaster, eavesdropping and information leakage come under information security threats.
Unchanged default password of any system comes under the category of vulnerabilities that the user may pose to its system.

g) Which of the following is **not** a proper method of maintaining confidentiality?

i. Biometric verification
ii. ID and password based verification
iii. 2-factor authentication
iv. switching off the phone

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT: Switching off the phone in the fear of preserving the confidentiality of data
is not a proper solution for data confidentiality.

h) Why would a hacker most probably use a proxy server?

i. To create a stronger connection with the target.
ii. To create a ghost server on the network.
iii. To obtain a remote access connection.
iv. To hide malicious activity on the network.

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT: Proxy servers exist to act as an intermediary between the hacker and the
target and server to keep the hacker anonymous.

i) What is the purpose of a Denial of Service attack?

i. Exploit a weakness in the TCP/IP stack
ii. To execute a Trojan on a system
iii. To shutdown services by turning them off
iv. To overload a system so it is no longer operational

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT: DoS attacks force systems to stop responding by overloading the processing of the system.

j) Which one of the following algorithms is not used in asymmetric-key cryptography?

i. RSA algorithm
ii. Diffie-Hellman algorithm
iii. ECC algorithm
iv. ECB algorithm

(02 marks)

ANSWER IN THIS BOX
(iv) CORRECT: Electronic Code Book algorithm is a block cipher method in which each block of text in an encrypted message corresponds to a block of data.

k) A unique piece of information that is used in any encryption system would be.

i. Cipher
ii. Plain Text
iii. Key
iv. Decipher

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: The key is the unique piece of information. It is used to create the cipher text and decrypt it back.

l) In public key cryptography, a key that decrypts the message is known as

i. Public Key
ii. Unique Key
iii. Private Key
iv. Random Key

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: Public key cryptography has 2 keys. They are private key and a public key.
The public key encrypts the message. The private key decrypts the message.

m) Which of these algorithms provides data integrity?

i. DES
ii. RSA
iii. SHA
iv. AES

(02 marks)

ANSWER IN THIS BOX
(iii) CORRECT: Hashing provides data integrity. Thus correct answer is SHA.

n) Which is the most secure way to remote login to a server?

i. SSH with public key
ii. SSH with password
iii. Telnet with password
iv. Telnet with public key

(02 marks)

ANSWER IN THIS BOX
(i) CORRECT: Telnet is inseure legacy protocol.
Asymmetric key based authentication is stronger than password.
Thus SSH with public key is the correct answer.

o) Kasun sends data to Jeewani. Chamath is sniffing the data transfer. In this given scenario, pick the closest in meaning to no-repudiation.

i. Jeewani can verify that the data was indeed sent by Kasun
ii. Chamath is unable to get the original data
iii. Kasun can verify if data reached Jeewani without any change
iv. Jeewani can verify if the data got changed by Chamath

(02 marks)

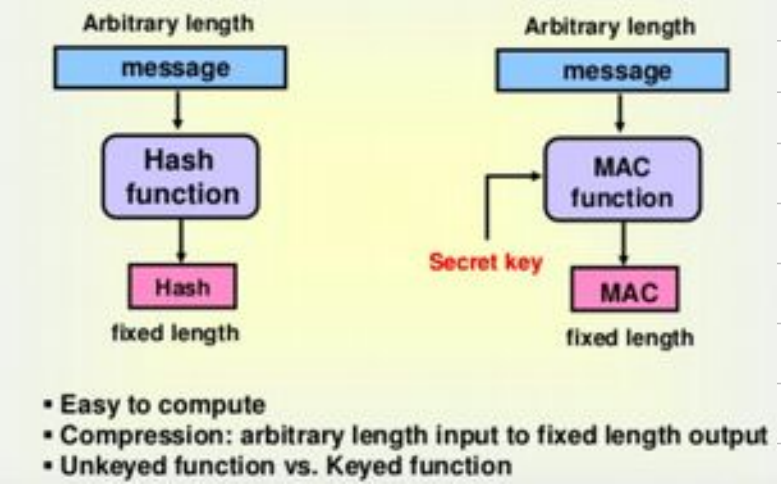
ANSWER IN THIS BOX
(i) CORRECT: Non-repudiation is the assurance that someone cannot deny his/her action.
Thus answer (i) is correct.

3) (a) Using a suitable diagram explain the differences between a **Hash** and a Message Authentication Code (**MAC**).

(06 marks)

ANSWER IN THIS BOX

The hash function is not keyed and MAC is keyed



(b) Compare and Contrast a computer **virus** and a **worm**.

(04 marks)

ANSWER IN THIS BOX

The primary difference between a virus and a worm is that viruses must be triggered by the activation of their host.

The virus doesn't spread itself. It needs a host and human help to spread.

Worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system.

(c) Distinguish between **Mandatory** and a **Discretionary** Access Control systems.

(04 marks)

ANSWER IN THIS BOX

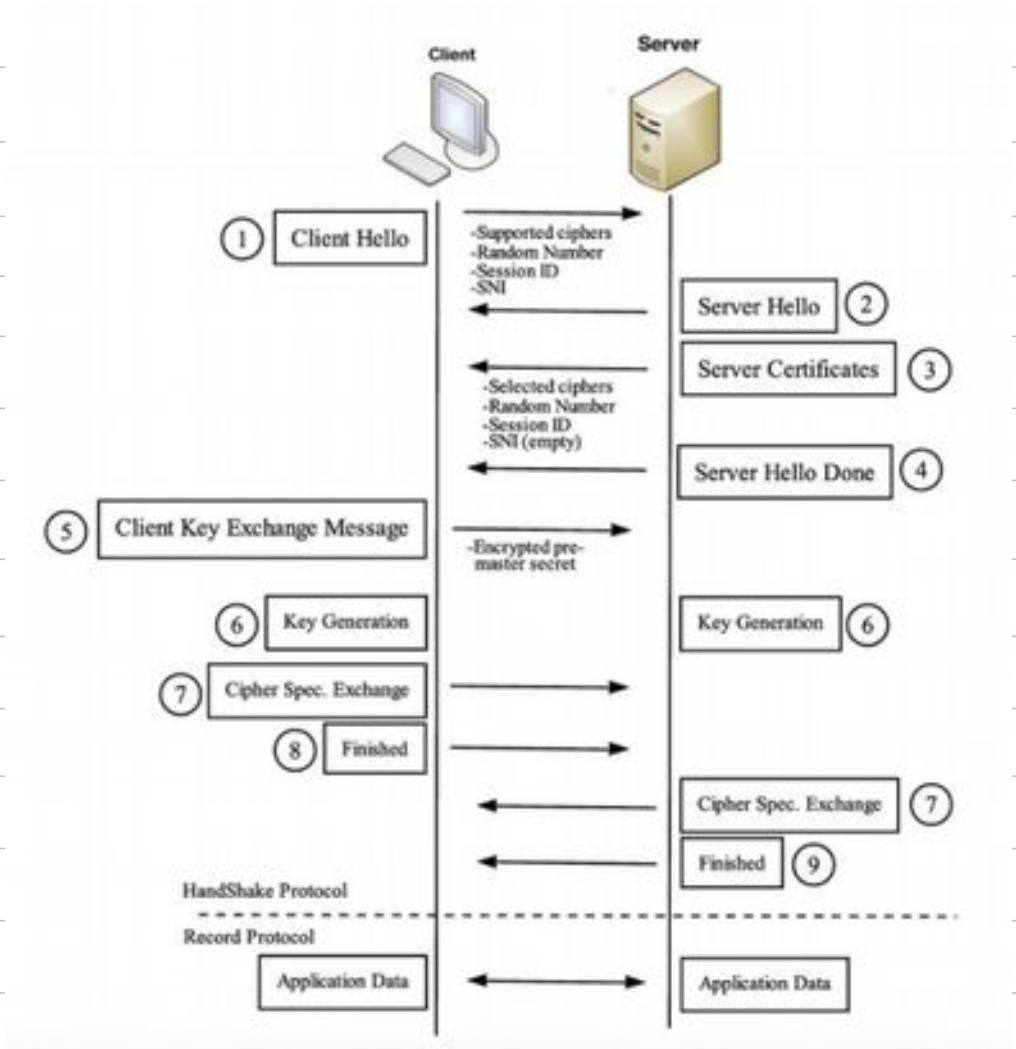
In mandatory access control (MAC), the system (and not the users) specifies which subjects can access specific data objects.

In discretionary access control (DAC), the owner of the object specifies which subjects can access the object.

(d) Explain the Transport Layer Security (TLS) handshake protocol by using a suitable diagram.

(06 marks)

ANSWER IN THIS BOX



4) a) Briefly describe the **fence** and **segmentation** methods which can be used to protect computer memory.

(04 marks)

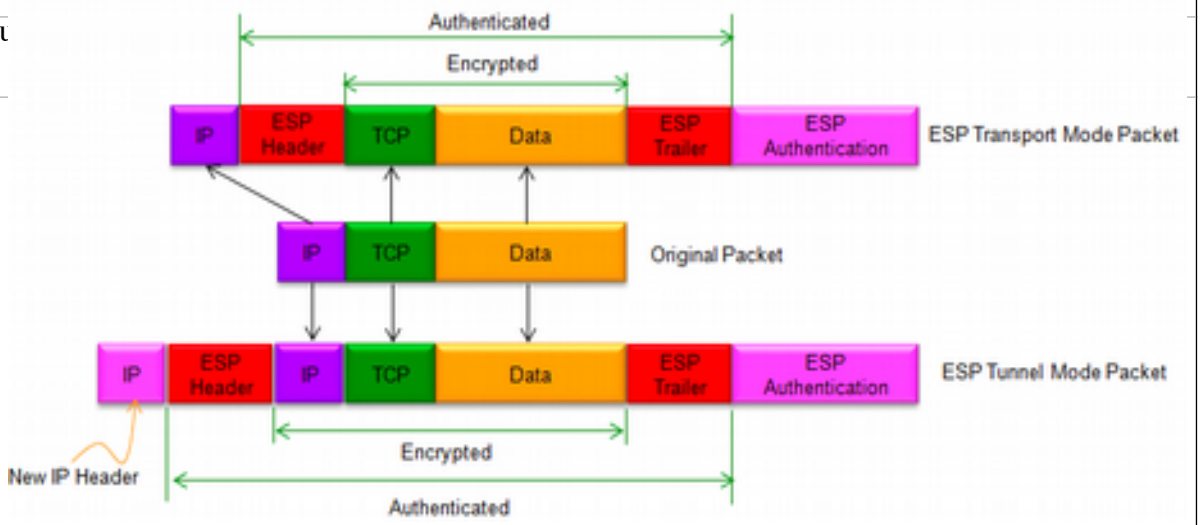
ANSWER IN THIS BOX
A fence is simplest form of memory protection which can be used only for single user operating system.
A fence is a particular address that users and their processes cannot cross.
Only the OS can operate on one side of the fence and users are restricted to the other side.
Segmentation refers to dividing a computer's memory into segments.
A reference to a memory location includes a value that identifies a segment and an offset within that segment.

b) 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 the IPSec ESP Tunnel Mode works to protect an IP datagram with a TCP payload.

(06 marks)

ANSWER IN THIS BOX

Stu



c) Describe the difference between an **Application Level** firewall and a **Packet Filtering** firewall?

(04 marks)

ANSWER IN THIS BOX

A packet filter firewall analyses network traffic at the transport protocol layer.

Packet filtering is the least secure firewall technology because it does not inspect the network packet's application layer data and does not track the state of connections.

An application level firewall evaluates network packets for valid data at the application layer before allowing a connection.

The firewall examines the data in all network packets at the application layer and maintains complete connection state and sequencing information.

d) Briefly explain the role of the human factor in information system security.

(06 marks)

ANSWER IN THIS BOX

Technology is quite an essential part relating to securing information assets but people are responsible for design, implementation and operation of these technological tools.

Human characteristics behaviour impacts information security and ultimately associated risks.

People will always be the most vulnerable part of any organisation's information security, because people make mistakes and they are easily manipulated.

****