107

UNIVERSITY OF COLOMBO, SRI LANKA

UCSC

University of Colombo School of Computing

BACHELOR OF SCIENCE IN INFORMATION SYSTEMS

Second Year Examination – Semester II – 2020/2021

IS 2109 – Information Systems Security (Part B)

TWO (2) HOURS (for both parts A & B)

To be completed by the candidate

Examination Index No: ....

Important Instructions to candidates:

1. The medium of instruction and question is **English**.
2. Write your answers in **English**.
3. If a page or a part of this question paper is not printed, please inform the supervisor immediately.
4. Note that questions appear on both sides of the paper. If a page is not printed, please inform the supervisor immediately.
5. Write your index number on each and every page of the answer paper.
6. This paper has **2** questions in **07** pages.
7. Answer **ALL** questions. All questions carry equal marks (**25** marks).
8. **This paper consists of two parts, Part A (Question No 1 and Question No 2) and Part B (Question No 3 and Question No 4) and submit separately.**
9. Any electronic device capable of storing and retrieving text including electronic dictionaries and mobile phones are not allowed.
10. **Non-Programmable** calculators are **allowed**.

For Examiner's use only	
Question No	**Marks**
1	
2	
3	
4	
Total	

Part B

Question 3

(a) Briefly explain the two terms 'Cryptography' and 'Cryptanalysis' with respect to Information Security.

[4 Marks]

(b) Briefly explain the following three (03) key components of a cryptosystem.

(i) Encryption algorithm

[2 Marks]

(ii) Decryption key

[2 Marks]

(iii) Cipher text

[2 Marks]

(c)

(i) Given below is a cipher text that has been encrypted using Caesar's Cipher. Decrypt and find the plain text.

Plain text: **'XST WIGVIX QMWWMSR'**
Shifted by: +4

[3 Marks]

(ii) Briefly explain two (02) disadvantages of using Caesar's Cipher.

[4 Marks]

(d) Use the following table that indicates decimal substitutions for alphabetic characters to solve parts (i) and (ii) of the question (d).

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(i) Encrypt the following plain text into cipher text using the Vernam Cipher. Clearly indicate the intermediary steps taken during the encryption process.
Plain text: 'ENCRYPTION'
Key stream: 70 58 87 04 51 28 59 11 00 08

[4 Marks]

(ii) The following cipher text has been encrypted using the Vernam Cipher. Decrypt it and generate the plain text. Clearly indicate the intermediary steps taken during the decryption process.
Cipher text: 'KRWQHSFQED'
Key stream: 03 13 11 05 18 21 16 24 18 00

[4 Marks]

Question 4

(a) In block ciphers, encryption can be done in different modes. **Illustrate** and briefly explain how encryption in the Cipher Block Chaining mode is implemented.

[6 Marks]

(b)

(i) Briefly explain two (02) applications of Hash functions.

[4 Marks]

(ii) Briefly explain how the integrity of a message can be ensured between the sender and receiver using the Message Authentication Code (MAC).

[3 Marks]

(c) Alice and Bob are communicating over a network that uses RSA, which is a public key algorithm. Use the below values to answer parts (d)(i) to (d)(iii) in question 4.

	Alice	Bob
Public Key	(5,39)	(3,33)
Private key	(5,39)	(7,33)

(ii) Alice wants to send the message '5' (M = 5) to Bob. What would be the cipher text (C) received by Bob? Clearly indicate the intermediary steps taken for the calculation.

[4 Marks]

(iii) Alice wants to send the message '2' (M=2) to Bob but she also wants to attach her digital signature to preserve the authenticity of her message. Use RSA to calculate her signature and clearly indicate the intermediary steps taken for the calculation.

[4 Marks]

(iii) Bob received a cipher text from Alice that says '6' (C=6). What would be the plain text?

[4 Marks]

****