





UCSC

UNIVERSITY OF COLOMBO, SRI LANKA

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.

1	niner's use nly
Question No	Marks
.1.	
2	
3	
4	
Total	

		 	 	 	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	-,	 	1
Index	No:	 	 	 			 ٠.	

Part B

1		4:0		3
V	ues	uo	ш	J

			akiran da balan ka balan da balan da balan balan balan balan balan da balan da balan da balan da da da da da d A	مياسي الأفاهات والا بد مطالحات به الإمامية بالأولامية الا الأولامية الأولامية بالا الأدامية الا
	m kanad ang kanada ang pangka mangka mangka M			
7,500,000,000	na sa Academia ya ya ya ye ya sa			
	nes d'inner de la comp			
				of this light is decreased in the house section in the light and the light of the l
	T I I II I			
1				
	Plant alphabet in the same or program		فيد المراجع والمراجعة	
	POLON BER SERVICE SERV			
	Briefl	ly explain the following three (03) key components of	a cryptosystem.	
	Briefl	ly explain the following three (03) key components of Encryption algorithm	a cryptosystem.	f2 Mark
			a cryptosystem.	[2 Mark
			a cryptosystem.	[2 Mark
			a cryptosystem.	[2 Mark
			a cryptosystem.	[2 Mark:
		Encryption algorithm	a cryptosystem.	[2 Mark
		Encryption algorithm	a cryptosystem.	
	(i)	Encryption algorithm	a cryptosystem.	[2 Marks

(iii)	Cipher text
a of all the last fine the same than be made in projects and same	
g while and distribute then then then then then then the or the property than the second	
g affek til e fillerinn ståreliger om, på pringstop, viljerige med, fyll der som	
L	
(i)	Given below is a cipher text that has been encrypted using Caesar's Cipher. Decrypt a find the plain text.
	Plain text: 'XST WIGVIX QMWWMSR'
	Shifted by: +4
	[3 Mar
planting of participates of the standard data had go being	
may magasi and for an after 1 the 164 of 26 ft ft, myst ft ft ft has been derived	
all of the literature of the annual contents of annual con-	
art our selection to the complete speciment part and page 1 graph grand page 1 grand (100 grand).	
(ii)	Briefly explain two (02) disadvantages of using Caesar's Cipher.
	[4 Mark

tradition of recommendate across an extra across as grass	
والمراقب المساورة والمراقبة والمراقبة والمراقبة والمراقبة والمراقبة والمراقبة والمراقبة والمراقبة والمراقبة وا	
PA in Paper and in a graph to be the consequence of the consequence	
entraga en en en el en el mes des els nerves de des els estragos en estragos els estragos en el estragos el est	

Index No:

OWOUND DESIGNATION OF THE PROPERTY OF THE PROP	SDW990W9eptawsos	CORRECTION CONTRACTOR	ORDOWNSDAMED COST	ORGENIO GRADANINO DE COMPENSOR	000000000000000000000000000000000000000	necessaries de la constitución d	recession.
Index	No:	4 2 4					

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

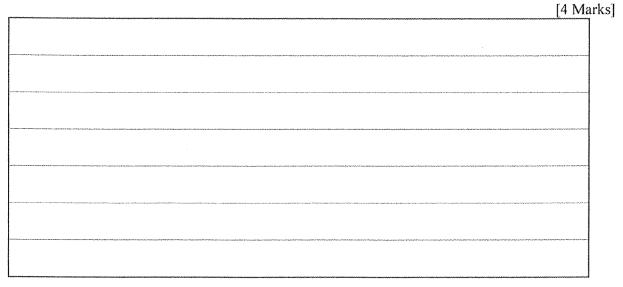
			700000										
A	В	С	D	Е	F	G	Н	I	J	K	L	M	1
00	01	02	03	04	05	06	07	08	09	10	11	12	
								-,					

		···		·								
N	O	P	Q	R	S	Т	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'

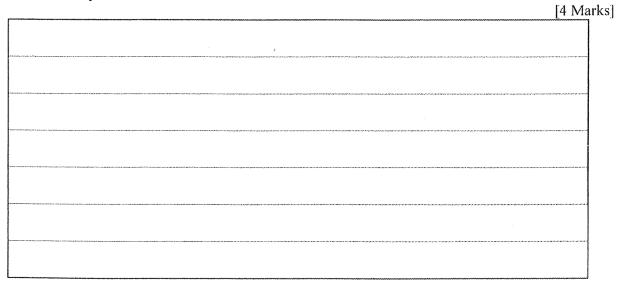
Key stream: 70 58 87 04 51 28 59 11 00 08



(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



Ques	ction 4	
(a)	In block ciphers, encryption can be done in different modes. Illustrate encryption in the Cipher Block Chaining mode is implemented.	
		[6 Marks
J-n		
)	(i) Briefly explain two (02) applications of Hash functions.	
		[4 Marks]
		P Note of No. 2 March 18 Physics of the State (18 Physics of the State
		a Principal de la digital de la principal de la principa de la principa de la principa de la principa de la pr

(b)

Index No:

				Index No	, 4 , , , , , , , , , , , , , , , , , ,	*********
ii)	Briefly receive	explain how the is r using the Message	ntegrity of a messa e Authentication Co	ige can be ensui de (MAC).	red between	the sende
						[3 M
-(transferrately distribution of the second section of the section of the second section of the section of the second section of the s	all for any service of the service between a graph and a series as the strate process, who are a series by Grab and series as	والمعارضة		we have the set of the second	s Norther Facilitation by Commission and Association agree (etc., by agreement, com-
		territor escribito esta de cambrica esta esta esta esta esta esta esta est	والمرافقة والمرا		ما المعادلة	t the late of the special particular state of the special contemperature and season may be.
	an particular and an investigal province by the space against an early and	to design of the tracking state of the first to the country to the tracking state that the bounds also by a fact of the	والمنافذة والمنا	addeler dy tan dy tro dae dae de gelfyd ei mae gan ar enwyt yn troed a gan y ag fair bei dy'r	51 (1/14 PT 1 1 54 SEC 1 1 1 55 SEC 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	The Mark Marks also refer to a set of the first fact the half below the related to the representative set of the
*************	Planting and the state of the s					
				ere betre fill det et de system fre dy den harfal in 1915 de 1915 de 1916 de 1916 de 1916 de 1916 de 1916 de 1	n marayanin dan dayari da maraya karaya karaya ya karaya ya karaya ya karaya ya karaya ya karaya ya karaya kar	a Parish ing Sanah danah san Balang ata ing kacamatan naggarah mag
***************************************	an and in the company of the pro-photocol terms are the pro-photocol to the order		ertern det in tim mellet de within som at vons de en mellet in de digt is, his hojd elephiske lichten je te is, beskyt		m Navana di Amerika Marana di Angalaya i Marana di Angalaya ing matang kanana sa da kanana sa da kanana sa da	an iku iyaa taa ina ka gil an ina galaan ka galaan iya ayaa iya ayaa iya ayaa iya iya iya
	danna mara pyryddig ar Thaddi'i glydyd rawrif arab ha demok	on employed an analysis by the spirit spirit of the spirit	The his high high in distributions contains and and private page is stored by place trips have all being right as by place		ermera och med med med det forskallen en delen skyrler, kvigar det en er nach en deten som en	المراد المراد والمراد والمراد المراد
			·····································	a trades in term respective part of the interest, and parties to a thirt deliver best on the chart of a total	t the first of the field decision for four for the engine give, the polygon republic of the engine give the first of the engine give give the engine give give give give give give give giv	than the change the play and an all a conservation constitutions are as the play and as

lice	and Rob	are communicating	avor a natival that	DCA 1:	1 ' 11'	
lice se th	and Bob	are communicating values to answer par	over a network that rts (d)(i) to (d)(iii) in	uses RSA, whic question 4.	h is a public	key algori
lice se th	and Bob	values to answer par	over a network that rts (d)(i) to (d)(iii) in	uses RSA, which question 4.	h is a public	key algori
lice se th	and Bob	Public Key	rts (d)(i) to (d)(iii) ir	1 question 4.	h is a public	key algori
lice se th	and Bob	values to answer par	rts (d)(i) to (d)(iii) in	1 question 4.	h is a public	key algori
se tr	ie below	Public Key Private key	Alice (5,39) (5,39)	Bob (3,33) (7,33)		
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text
se tr	Alice w	Public Key Private key	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text
lice se th	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.
se tr	Alice w	Public Key Private key rants to send the me	Alice (5,39) (5,39) essage '5' (M = 5)	Bob (3,33) (7,33) to Bob. What w	ould be the	cipher text lation.

(c)

(iii)	signature to preserve the authenticity of her message. Use RSA to calculate and clearly indicate the intermediary steps taken for the calculation.	[4 Ma
***************************************		[4 1714]
energia de la composito de la		
anarana venarana antika		a a photograph high logache by the play low op playing and (post by a bentile 1978) to
		il militare tende ceritoria en en escara en escara con en tende en el tende de el tende de el tende de el tend
No. 20 6 7 6 7 7 10 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		
aminga na kao kaomin' na kaopin		l and an'i di serimber a haracteris construction and construction, we construct a serimber has been been designed.
iii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
iii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	he plain text' [4 Mar
iii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
iii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
ii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
ii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
ii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
iii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
ii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
iii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
ii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
iii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
iii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
ii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
ii)	Bob received a cipher text from Alice that says '6' (C=6). What would be t	
	Bob received a cipher text from Alice that says '6' (C=6). What would be t	

Index No: