

UNIVERSITY OF COLOMBO, SRI LANKA



UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

BACHELOR OF SCIENCE IN COMPUTER SCIENCE
BACHELOR OF SCIENCE HONOURS IN COMPUTER SCIENCE
BACHELOR OF SCIENCE HONOURS IN SOFTWARE ENGINEERING
Third Year Examination – Semester I – 2017

SCS 3106 — Information System Security TWO (2) HOURS

To be completed by the candidate

Examination Index No:

Important Instructions to candidates:

- 1. The medium of instruction and questions is English.
- Note that questions appear on both sides of the paper. If a page or a part of the question paper is not printed, please inform the supervisor immediately.
- 3. Write your index number on each and every page of the question paper.
- 4. This paper has **04** questions in **16 pages**.
- Any electronic device capable of storing and retrieving text including electronic dictionaries and mobile phones are not allowed.
- 6. Calculators are not allowed.

For Examine	er's use only
Question No	Marks
1	
2	
3	
4	
Total	

***************************************			[4 mark
	ber []		
b). Define th	ne following conce	epts using one sentence each: (i) Attack, (ii) Vulro information security.	nerability and
b). Define th	ne following conce ats with respect to	epts using one sentence each: (i) Attack, (ii) Vulro information security.	
o). Define th (iii)Threa	ne following conce ats with respect to	epts using one sentence each: (i) Attack, (ii) Vulro information security.	nerability and [6 mark
o). Define th (iii)Threa	ne following conce ats with respect to	o information security.	[6 mark
o). Define th (iii)Threa	ne following conce ats with respect to	epts using one sentence each: (i) Attack, (ii) Vulro information security.	[6 mark
b). Define th (iii)Threa	ne following conce ats with respect to	o information security.	[6 mark
b). Define th	ne following conce ats with respect to	o information security.	[6 marl

	Index Number	
(c).	Explain briefly, the concept of one-way hash function.	
	fo market	[5 marks]
(d).	Describe how a one-way hash function may be used for message authentication	
		[5 marks]

			[5 mark

	to the Internet securit	-			[6 m
). Write down th	e outcome of the foll	lowing Javas	statement.		
	re Sig=Signatu			A1withDSA")	
					[5 m

1				

		[7 mark
		Į. mark

Index Number					
				Mal and	

- (a). Discuss the characteristics of credit card, digital cash and subscription payment methods with regard to the following properties.
 - i. The person who has the funds/money
 - ii. Time of payment vs time of order/shopping

[6 marks]

(b). Briefly explain th	e life cycle of a digital cash.	
[axiem T]		[5 n

	[7 mar	'ks

	Index Number			Borneid	xebhi	
Describe h	ow a man-in-the-middle	e attack m	av he ner	formed on a	TI C 2277	antina and the
consequenc	es of such an attack.	o attaon m	ay be pen	onneu on a	i LS conn	ection and the
reice it ko Selika e b	nadeno (3) revose enti- processi works i listo					[7 marks]
						ETOE D

Index Number				adm	old i

4. (a). i. Kerberos involves three message exchanges, one between the client (C) and the Key Distribution Center (KDC), one between the client and the Ticket Granting Service (TGS), and one between the client and the server (S) chosen by the client. Briefly explain how Kerberos authentication process works using a suitable diagram

[8 marks]

	[o manto]
	TOTAL HEIGHT -

[Zmerks]	Taxashari ni talinessa si notispiroti biya and vriw nistoxii bit
[anana]	Clever telliteration and the second of the s
	(2) IN THE PROPERTY OF THE PR

Index Number	
ii. Explain why time synchronization is essential in Kerberos?	[2 marks]
(b). i. What is a packet filter firewall?.	[4 marks]

	Index Num			1 160	0/1/9			
ii. What is t	tiny fragment	attack wh	ich was fou	und in p	acket filt	ering fire		
E E							[2 ma	rksj
				o-homo	d hastin	n config	uration	
ii Briefly ovr	Vain corponed	A DOCT TITOL	Malle, cibal				uralion.	
ii. Briefly exp	olain screened	nost fire	walls' singl	e-nome	a bacao			rks]
ii. Briefly exp	olain screened	nost fire	walis' singi	e-nome	a baono		[2 ma	rks]
ii. Briefly exp	olain screenec	d host fire	walls' singl	e-nome				rks]
ii. Briefly exp	olain screenec	d host fire	walls' singl	e-nome				rks]
ii. Briefly exp	olain screenec	d host fire	walls' singl	e-nome				rks]
ii. Briefly exp	olain screenec	d host fire	walls' singl	e-nome	04 (8)			rks]
ii. Briefly exp	olain screened	d host fire	walls' singl	e-nome	() (E) (rks]
ii. Briefly exp	olain screened	d host fire	walls' singl	e-nome	qq1 (C) 1			rks]
ii. Briefly exp	olain screened	d host fire	walls' singl	e-nome	(N. (C.)			rks]
ii. Briefly exp	olain screened	d host fire	walls' singl	e-nome	(14 (8))			rks]
ii. Briefly exp	olain screened	d host fire	walls' singl	e-nome				rks]
ii. Briefly exp	olain screened	d host fire	walls' singl					rks]
ii. Briefly exp	olain screened	d host fire	walls' singl	e-nome	q.4. (8) a			rks]
ii. Briefly exp	plain screened	d host fire	walls' singl	e-nome	Q41 (E) 1			rks]
ii. Briefly exp	plain screened	d host fire	walls' singl	e-nome				rks]
ii. Briefly exp	plain screened	d host fire	walls' singl	e-nome				rks]
ii. Briefly exp	plain screened	d host fire	walls' singl	e-nome				rks]

	Index Number	Sca Lari Scar
(c). IPSec op the differ	perates on two (2) modes called trainence between them?	nsport mode and tunnel mode. What i
		[4 marks
d). Write dov	wn three (3) types of intruders.	[2 marks]
		[3 marks]