



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**.
2. 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.
5. Any electronic device capable of storing and retrieving text including electronic dictionaries and mobile phones are **not allowed**.
6. Calculators are **not allowed**.

For Examiner's use only

Question No	Marks
1	
2	
3	
4	
Total	

--	--	--	--	--	--	--	--

- [4 marks]

UNIVERSITY OF CALIFORNIA SCHOOL OF COMPUTING

BACHELOR OF SCIENCE IN COMPUTERS

BACHELOR OF SCIENCE HONORS IN COMPUTER SCIENCE

BACHELOR OF SCIENCE HONORS IN SOFTWARE ENGINEERING

THIRD YEAR EXAMINATION - 2011-2012

2011-2012 - Information Systems 2011

Two (2) Hours

To be completed by the candidate

Examination Room No.

Examination Instructions

- [6 marks]

1992

Index Number

--	--	--	--	--	--	--	--

(c). Explain briefly, the concept of one-way hash function.

[5 marks]

--

(d). Describe how a one-way hash function may be used for message authentication.

[5 marks]

--

--	--	--	--	--	--	--	--

[5 marks]

Index Number

--	--	--	--	--	--	--	--

2. (a). Compare and contrast regular digital certificate and Extended Validation (EV) certificate with regard to the Internet security.

[6 marks]

--

- (b). Write down the outcome of the following Java statement.

`Signature Sig=Signature.getInstance("SHA1withDSA")`

[5 marks]

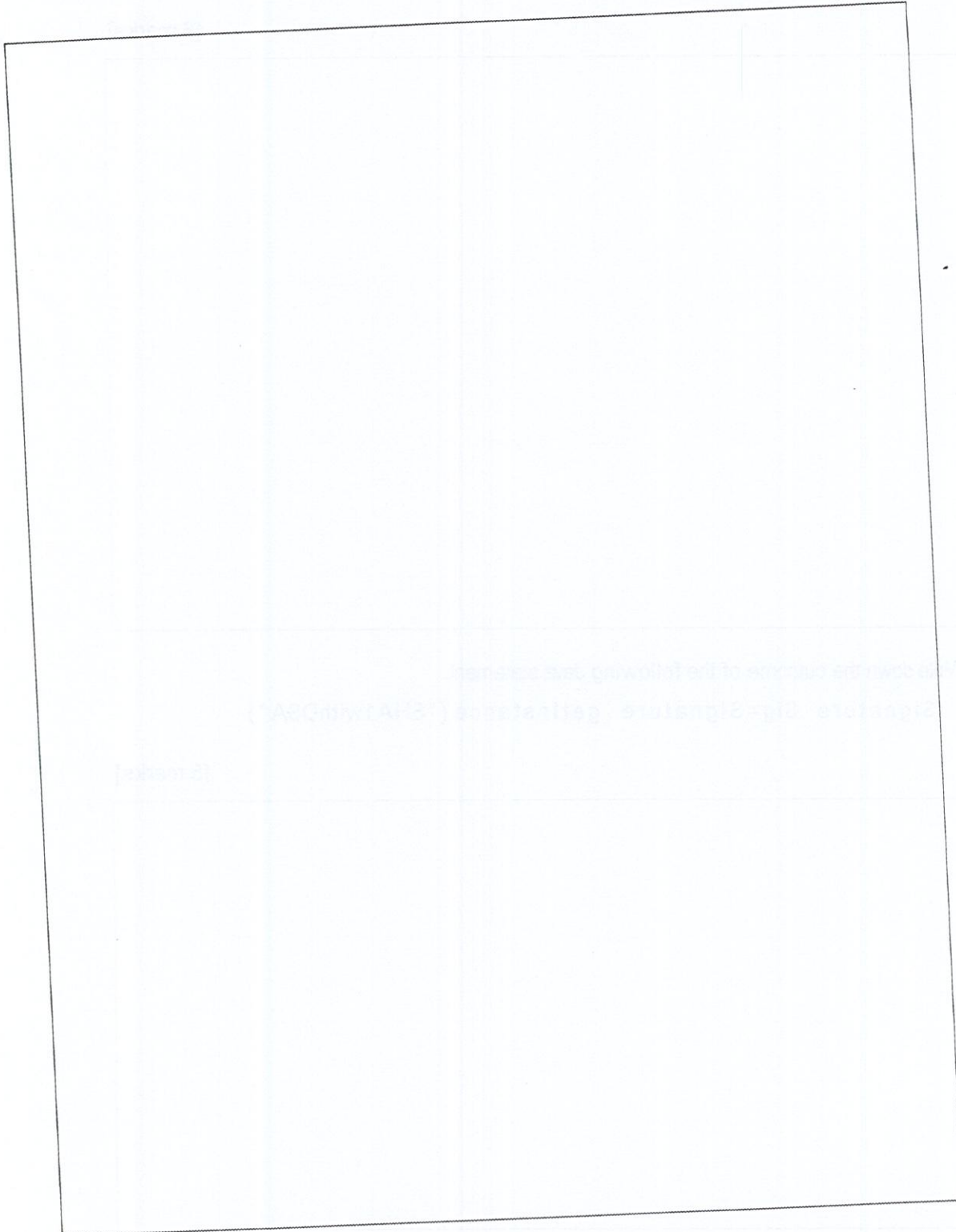
--

Index Number

--	--	--	--	--	--	--	--

(c). Explain how public key cryptography may be used for key distribution.

[7 marks]



--	--	--	--	--	--	--	--

- [7 marks]

Index Number

--	--	--	--	--	--	--	--

3. (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]

--

--	--	--	--	--	--	--	--

Index Number

--	--	--	--	--	--	--	--	--

- (c). What is a Blind Signature? Briefly explain the cut and choose protocol with regard to the blind signature.

[7 marks]

--

--	--	--	--	--	--	--	--

- [7 marks]

Index Number

--	--	--	--	--	--	--	--

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]



--	--	--	--	--	--	--	--

Index Number

--	--	--	--	--	--	--	--

ii. Explain why time synchronization is essential in Kerberos?

[2 marks]

--

(b). i. What is a packet filter firewall?.

[4 marks]

--

Index Number

--	--	--	--	--	--	--	--

ii. What is tiny fragment attack which was found in packet filtering firewalls?

[2 marks]

--

iii. Briefly explain screened host firewalls' single-homed bastion configuration.

[2 marks]

--

--	--	--	--	--	--	--	--

- [4 marks]

10

- [3 marks]

