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

Academic Year 2014/2015 - Third Year Examination - Semester 1 - 2015

SCS 3106 — Information System Security

(2 Hours)

Answer All Questions

Number of Pages = 12 Number of Questions = 4

To be completed by the candidate

Index Number | | | | | | | | |

Important Instructions

- The duration of the paper is **2** Hours.
- The medium of instruction and questions is English.
- This paper has **4** questions on **12** pages.
- Answer **all** the **4** questions.
- **Write your answers only on the space provided** on this question paper.
- Do not tear off any part of this answer book. Under no circumstances may this book (or any part of this book), used or unused, be removed from the Examination Hall by a candidate.
- 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.

To be completed by the examiners

1	
2	
3	
4	
Total	

Index Number | | | | | | | | |

1. (a). State the concepts of Authenticity, Integrity, Confidentiality, and Nonrepudiation with respect to information systems security.

[4 marks]

(b). Write down two(2) security methods that can be used to achieve data Integrity.

[4 marks]

Index Number | | | | | | | | |

(c). Decrypt the cipher text C = **khoor xfvf** which has been encrypted using the Caesar cipher with the security key K= **3**. What is the main drawback of the Caesar cipher?

[5 marks]

(d). Describe what is meant by a one-way hash function and show how a one-way hash function can be used to cryptographically protect a file with a passwords.

[6 marks]

Index Number | | | | | | | | |

(e). Suppose that one needs to use a stream cipher to share a real time audio streams. Describe a suitable block cipher operational mode that can be used for the above requirement.

[6 marks]

Index Number | | | | | | | | |

2. (a). Suppose the User **A** generates a cipher text C = EK2[DK2[EK1[P]]] where K1 and K2 are symmetric keys. Can the User **B** retrieve the plain text P= DK3[EK3[DK1[C]]] where K1 and K3 are symmetric keys. Justify your answer.

[5 marks]

(b). List two (2) advantages of asymmetric key cryptography.

[4 marks]

Index Number | | | | | | | | |

(c). Amal has the public key:$e = 23$, $n = 121879$ and the private key $d = 110639$, $n = 121879$. Bimal has the public key: $e = 17$, $n = 120979$ and the private key $d = 70753$, $n = 120979$.

Amal wants to encrypt a message: $M=4$ to Bimal and Bimal wants to sign the message: $N = 6$ to Amal. What messages will Bimal and Amal receive respectively?

[6 marks]

Bimal will receive:

Amal will receive:

(d). Explain what is meant by a Hybrid Encryption process and write down two (2) reasons to use it.

[5 marks]

Index Number | | | | | | | | |

(e). What is the purpose of a Certification Authority (CA)?

[5 marks]

Index Number | | | | | | | | |

3. (a). What is the purpose of the following Open SSL command?
openssl req -new -x509 -out host.pem -keyout key.pem
Which files will be created as the result of the command?

[6 marks]

(b). Explain a method that is used to perform authentication between a browser and a web server by using a asymmetric key cryptographic algorithm?

[7 marks]

Index Number | | | | | | | | |

(c). List five (5) best practices with regard to e-mail security.

[5 marks]

(d). What are the basic security services that S/MIME provides? Briefly explain how S/MIME provides these security services. What are the other e-mail security requirements that S/MIME does not provide?

[7 marks]

Index Number | | | | | | | | |

4. (a). List three (3) features assures to a router to defend against network layer attacks.

[6 marks]

(b). Using suitable diagrams, explain how ESP (encapsulating security payload) and AH (authentication header) helps to achieve transport and tunnel modes of IPSec. In your explanation, briefly highlight how integrity and confidentiality of IP datagrams is achieved in those two modes.

[5 marks]

Index Number | | | | | | | | |

(c). Explain four (4) guidelines for properly setting up IPSec in order to avoid pitfalls of IPSec misconfiguration.

[4 marks]

(d). Briefly explain three (3) attacks which can occur against packet filtering firewalls and mention a countermeasure for each attack.

[6 marks]

Index Number | | | | | | | | |

(e). Briefly explain how probe requests from WiFi client devices can be used by attackers to reveal information of the personal life of device owners.

[4 marks]

****