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 in Computer Science - First Semester

Academic Year 2015/2016

SCS 3106 — Information System Security

(2 Hours)

Answer All Questions

Number of Pages = 11 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 **11** 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 **Kerckhoff Principle**.

[4 marks]

(b). Define the terms **Unconditional Security** and **Computational Security** with respect to the cryptographic algorithms.

[4 marks]

(c). State the concepts of **Authentication**, **Authorization** and **Accountability** with respect to information systems security.

[6 marks]

Index Number | | | | | | | | |

(d). Briefly describe three (3) security controls that can be used to provide the data **confidentiality**.

[6 marks]

(e). i. Decrypt the cipher text C = **0111 1110 1010 1101** which has been encrypted using the Vernam cipher with the security key K= **0001 0001 1111 1110**.

ii. What is the main drawback of the Vernam cipher?

[5 marks]

Index Number | | | | | | | | |

2. (a). Explain why a stream cipher fails to protect message integrity.

[6 marks]

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

[6 marks]

Index Number | | | | | | | | |

(c). What are the length of ciphertexts when eight(8) bytes and eighteen (18) bytes of plaintext are encrypted in DES and AES ciphers with ECB mode.

[6 marks]

(d). The four basic modes of operations of a block cipher (ECB, CBC, OFB, CFB) are analysed with respect to error propagation in encryption. For the sequence of ciphertext blocks (c_1; c_2; c_3; ... ; c_n), ciphertext block c_j is errorness (1 <j <n). Specify which of plaintext blocks (x_j; x_{j+1}; x_{j+2}; ... ; x_n) are received incorrectly.

[7 marks]

Index Number | | | | | | | | |

3. (a). Describe the RSA (Rivest Shamir and Adelman) public key cryptographic algorithm. Your answer should include

i. The generation of public and private keys
ii. The encryption algorithm
iii. The decryption algorithm

[6 marks]

(b). What is the purpose of a Public Key Infrastructure (PKI)?

[6 marks]

Index Number | | | | | | | | |

(c). What is the purpose of the following Open SSL command? Which files will be created as the result of the command?

openssl req -new -nodes -out req.pem -keyout key.pem

[6 marks]

(d). What are the basic security services that PGP provides? Briefly explain how PGP provides these security services by using a appropriate diagram.

[7 marks]

Index Number | | | | | | | | |

4. (a). i. Briefly explain two (2) fundamental weaknesses in **WEP (wireless equivalent privacy)** protocol used in wireless LANs (WiFi) and how they are eliminated in IEEE 802.11i/WPA2 later. Your explanation should clearly state how those problems are solved in the new protocol.

[4 marks]

Index Number | | | | | | | | |

ii. Imagine a coffee shop where a free WiFi network with ESSID called 'SiraCoffee' is available protected by WPA2 protocol. You are a visitor to that place with a WiFi enabled laptop running Wireshark software and a 3G dongle with mobile Internet access. Briefly explain how you will be setting up a bogus AP within the coffee shop to drive other peoples IP packets through your laptop to see their data while not interrupting their web browsing capability.

[8 marks]

Index Number | | | | | | | | |

(b). IPSec is a framework for securing IP packets sent through the public Internet. Depending on the amount of security we need, it is possible to configure IPSec in different ways. **IPSec ESP (Encapsulating Security Payload) Tunnel Mode** is such a configuration. Using a suitable diagram,explain how IPSec ESP Tunnel Mode works to protect an IP datagram with a TCP payload.

[8 marks]

Index Number | | | | | | | | |

(c). Availability of cheap **Software Defined Radio (SDR)** hardware enables people to access frequencies where proprietary communication protocols are used with licenses. Discuss the wireless network security challenges that can arise in the future when hobbyists with cheap SDR devices start sniffing currently restricted areas in the wireless spectrum. (*Your answer should assume that the frequency range available for an SDR device is from 10MHz to 6GHz.*)

[5 marks]

****