University of Colombo, Sri Lanka

UCSC *University of Colombo School of Computing*

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

Academic Year 2021/2022 — Semester II

SCS 2214 — Information Systems Security

(2 Hours)

Answer All Questions

Number of Pages = 13 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 instructions and questions is English.
- This paper has **4** questions on **13** pages.
- Answer **all 4** questions.
- **Write your answers on and 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.
- Any electronic device capable of storing and retrieving text, including electronic dictionaries and mobile phones, are **not allowed**.
- Non-programmable Calculators may be used.

To be completed by the examiners

1	
2	
3	
4	
Total	

Index Number | | | | | | | | |

1. (a). Define the following terms with regard to Information Systems Security: **Vulnerability, Attck, Control, Problem, Threat** and the **Risk.**

[6 marks]

(b). Define four (4) fundamental protection method to archive confidentiality of information.

[4 marks]

Index Number | | | | | | | | |

(c). Show how Vernam cipher works by using a suitable example. Also state under which conditions is the Vernam cipher unconditionally secure?

[4 marks]

(d). Show how the DES block cipher can be used to build a 64-bit hash function.

[5 marks]

Index Number | | | | | | | | |

(e). Design a one-time password scheme by using a secure hash function.

[6 marks]

Index Number | | | | | | | | |

2. (a). Which mode of operation of the Advanced Encryption Standard (AES) block cipher would you use to protect the following? Give a brief justification for your answers.

i. Inter-bank funds transfers.

[2 marks]

ii. Email messages.

[2 marks]

iii. A high-frequency radio communication link.

[2 marks]

iv. The signal from a gearbox sensor to the central control unit in a truck.

[2 marks]

Index Number | | | | | | | | |

(b). Show how Triple DES encryption method works by using a suitable diagram. Explain the reasons to use Triple DES over Double DES method.

[7 marks]

Index Number | | | | | | | | |

(c). Suppose we want to use the RSA algorithm between two end points, **A** and **B**, and we have chosen (27,55) as public key of **B** and (41,133) as private key of **A**.

i. **A** has a message **M**=5 to be sent to **B**. What is the signature **S** of message **M**?

[4 marks]

ii. **A** encrypts the message **M**=10 and signature **S** above in (i) before it transmits to **B**. What is the cipher text of message **M** and signature **S**?

[6 marks]

Index Number | | | | | | | | |

3. (a). Amali and Buddhika participate in a public-key infrastructure that enables them to exchange legally binding digital signatures.

i. Name two reasons why, for some purposes, Amali might prefer to use a message authentication code, instead of a digital signature, to protect the integrity and authenticity of her messages to Buddhika.

[4 marks]

ii. Outline a protocol for protecting the integrity and authenticity of Amali's messages to Buddhika that combines the benefits of a public-key infrastructure with those of using a message authentication code.

[4 marks]

Index Number | | | | | | | | |

(b). Compare and contrast the usability and security of messaging using encrypted email (either GPG or SMIME) and end-to-end encrypted messaging apps (WhatsApp, Signal, or iMessage).

[7 marks]

Index Number | | | | | | | | |

(c). You are responsible for designing, implementing and maintaining a user authentication and data encryption service for a new e-commerce website. The website will include a market-place for third party vendors, multiple methods of processing payments and is optimised for mobile and desktop computers. Describe and justify your design with details.

[10 marks]

Index Number | | | | | | | | |

4. (a). "Virtual Private Networks are not necessarily confidential"
State if the above statement is true or false and justify your answer by using examples.

[5 marks]

(b). Describe an information security violation of Data Leakage Protection (DLP) implemented in Next Generation Firewalls / Unified Threat Management (UTM) devices by using an example.

[5 marks]

Index Number | | | | | | | | |

(c). Explain two (03) benefits of using Host based Intrusion Detection Systems (HIDS) over Network based Intrusion Detection Systems (NIDS).

[6 marks]

(d). Write four (04) features of Unified Threat Management (UTM) devices.

[4 marks]

Index Number | | | | | | | | |

(e). "Keeping the salt value of a password in the same database table in plain text is acceptable" State if the above statement is true or false and justify your answer.

[5 marks]

****