060

University of Colombo, Sri Lanka

University of Colombo School of Computing

BACHELOR OF SCIENCE IN COMPUTER SCIENCE

Second Year Examination - Semester II - UCSC AY20 [held in March/April 2024]

SCS 2214 — Information System Security

Two (2) Hours

Answer All Questions

Number of Pages = 10 Number of Questions = 4

To be completed by the candidate

Index Number | | | | | | | | |

Important Instructions to candidates

- Please ensure that you have received the correct examination paper.
- Students should answer in the medium of **English language only** using the space provided in this question paper.
- Note that questions appear on both sides of the paper. If a page or a part of this question paper is not printed, please inform the supervisor immediately.
- Write your index number **CLEARLY** on each and every page of this Question paper.
- This paper has **4** questions on **10** pages (including the Cover Page).
- The duration of the paper is Two (02) Hours.
- Answer **all 4** questions.
- 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.
- **Write your answers on and only on the space provided** on this question paper.
- Calculators and any electronic device capable of storing and retrieving text including electronic dictionaries, smart watches 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). Explain the main difference between an **Amateur** and a **Cracker** with respect to cyber attack.

[5 marks]

(b). What is meant by a Message Authentication Code (MAC) algorithm? List three(3) fundamental requirements of a MAC algorithm.

[6 marks]

Index Number | | | | | | | | |

(c). Block ciphers usually process 64-bit or 128-bit blocks at a time by using a block cipher operational mode. Cipher Feed Back (CFB) mode and Output Feed Back (OFB) mode are such operational modes.

i. Briefly explain the reason for using these two operational modes.

[4 marks]

ii. Briefly describe differences between OFB mode and CFB mode.

[4 marks]

(d). Explain a method to prevent a **Dictionary Attack** with regards to password based authentication.

[6 marks]

Index Number | | | | | | | | |

2. (a). Briefly explain the **PKCS5 Padding** Scheme by using a suitable diagram.

[5 marks]

(b). Determine the Greatest Common Divisor (GCD) of 23465 and 12340.

[5 marks]

(c). Suppose we want to use the RSA algorithm between two end points, **A** and **B**, and we have chosen p =11 and q=7.

i. **A** has chosen private key d as 43. Calculate the public key of **A**?

[3 marks]

Index Number | | | | | | | | |

ii. **A** has a message **M**=2 to be sent to **B**. What is the signature **S** of message **M**?

[3 marks]

iii. **B** encrypts the message **M**=3 before it transmits to **A**. What is the cipher text of message **M**?

[3 marks]

(d). Suppose we want to use the Diffie-Hellman Key Agreement protocol between two parties, A and B, and we have chosen the integer g=6 and the integer n=13. If A generates the private key x=5 and B generates the private key y=4, calculate the session key k between A and B.

[6 marks]

Index Number | | | | | | | | |

3. (a). Explain the purpose of a Certificate Authority (CA) in public key infrastructure (PKI).

[6 marks]

(b). Compare and contrast **SMIME** and **PGP** e-mail security standards over a public key distribution.

[6 marks]

Index Number | | | | | | | | |

(c). Explain the security operations of PGP by using a suitable diagram.

[6 marks]

(d). Explain the concept of Blockchain with respect to the Bitcoin protocol.

[7 marks]

Index Number | | | | | | | | |

4. (a). Password Authentication Protocol (PAP) is an obsolete protocol where Challenge Handshake Authentication Protocol is vulnerable if not implemented correctly. Kerberos is a protocol that is used to authenticate both clients and services in an open (insecure) network.

i. Describe the mechanism used by Key Distribution Center (KDC) to share a key between a client and a service.

[7 marks]

ii. Describe authentication by direct presentation and explain why it is not suitable for open networks.

[3 marks]

Index Number | | | | | | | | |

iii. List the factors considered for authentication and write one weakness for each of those factors.

[3 marks]

(b). Write four (04) variants of available IP Security protocols and write a single sentence (no more than 20 words) to explain the variant you wrote.

[12 marks]

Index Number | | | | | | | | |

****