152



# University of Colombo, Sri Lanka

*University of Colombo School of Computing*

**BACHELOR SCIENCE IN COMPUTER SCIENCE**

Second Year Examination in Computer Science - Second Semester

Academic Year 2019/2020

## SCS 2214 — 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.
- Write your answers in 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). Briefly state the concepts of **Confusion** and **Diffusion** with respect to Cryptographic Algorithm.

**[4 marks]**

(b). i. State the Kerckhoffs' principle.

ii. Briefly describe importance of this principle with an example.

**[4 marks]**

**Index Number** | | | | | | | | |

(c). Suppose we have nodes A, B, C, D and E in a point to point network. How many keys do we have to generate such that A, B C,D and E can communicate with each other in a bidirectional secure way using the 3DES encryption algorithm.

**[3 marks]**

(d). Calculate the length of hash when the message length is sixteen (16) bytes with respect to the following Hash algorithms.

i. SHA-1
ii. SHA-256
iii. MD5

**[3 marks]**

(e). Calculate the length of cipher text message when the plain text message length is nineteen (19) bytes with respect to the Advanced Encryption Standard (AES) algorithm when operate it in the following modes.

i. Cipher Block Chaining (CBC) mode
ii. Output Feedback(OFB) mode

**[4 marks]**

**Index Number** | | | | | | | | |

(f). i. Encrypt the message M = **HELLOUCSC** by using the Kamasutra cipher with the security key K= **G H A J R I O B E S Q C L F V Z T Y K M X W N U D P.**

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

**[7 marks]**

**Index Number** | | | | | | | | |

**2.** (a). Show how a one-way hash function can be converted to a Message Authentication Code (MAC).

**[6 marks]**

(b). Suppose that one needs to use a block cipher to encrypt a video call. Describe a suitable block cipher operational mode that can be used for the above requirement.

**[6 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 A and (3,55) as private key of A.

i. A has a message M=13 to be sent to B. What is the signature S of message M?

ii. B has a message M=10 to be sent to A. What is the cipher text C of message M?

**[8 marks]**

(d). Describe TLS authentication protocol.

**[5 marks]**

**Index Number** | | | | | | | | |

3. (a). You were consulted for a datacenter implementation project and network engineers ask you to recommend solutions considering their requirements. Carefully read following requirements before answering the questions.

IPSec Virtual Private Network (VPN) should be configured for software developers to access client's pre-production site deployed in a De-Mileterised Zone (DMZ). The connectivity should support Network Address Translation (NAT). A defined network from software developers company will be allowed to access pre-production DMZ.

i. What IP Security **communication mode** you recommend for the above requirement?

**[3 marks]**

ii. What IP Security **protocol type** you recommend for the above requirement?

**[3 marks]**

iii. Explain how NAT is possible with the recommended IP Security protocol type compared to the other IP Security protocol type?

**[8 marks]**

**Index Number** | | | | | | | | |

iv. Write down five (05) features that are available in Unified Threat Management (UTM) appliance?

**[5 marks]**

v. Write down three (03) limitations of firewalls?

**[3 marks]**

vi. Explain what following `iptables` rule does?

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
```

**[3 marks]**

Index Number | | | | | | | | |

4. (a). Kerberos is a protocol that is used to authenticate both clients and services in an open (insecure) network.

i. Explain the functionality of the Kerberos protocol using a diagram.

**[6 marks]**

ii. Describe how Kerberos protocol allows a client to verify authenticity of a service.

**[8 marks]**

Continued ...

**Index Number** | | | | | | | | |

(b). Malicious internal users can do considerable damage to an organization or individuals of the organization if the network is not well protected against such attacks.

i. Explain how Dynamic Host Configuration Protocol (DHCP) spoofing can be a severe insider attack?

**[6 marks]**

**Index Number** | | | | | | | | |

ii. Describe FIN scan using a diagram?

**[5 marks]**

_____ ********** _____