The Open University of Sri Lanka
Faculty of Engineering Technology
Department of Electrical & Computer Engineering

242

Study Programme	: Bachelor of Software Engineering Honours
Name of the Examination	: Final Examination
Course Code and Title	**: EEI5270 Information Security**
Academic Year	: 2023/2024
Date	: 11th August 2024
Time	: 1330 - 1630 hrs
Duration	: **Three(3) hours**

General Instructions

- Read all instructions carefully before answering the questions.
- This paper consists of **Four(4)** questions in Two(2) pages.
- Answer **ALL** Questions. All questions carry equal marks.
- Answers for each question should commence from a new page.
- Try to write answers in **point form**.
- This is a **Closed Book Test(CBT)**.
- Answers should be in clear hand writing.
- Do not use any colour pen other than **blue/black**.
- **General Examination Guidelines of the OUSL are applicable**.

QUESTION 1

1.1) Differentiate between **data** and **information**.

(3 marks)

1.2) Briefly explain the following key goals of information security.

i) Confidentiality
ii) Integrity
iii) Availability

(6 marks)

1.3) Briefly describe the following terms in relation to information security:

i) Threat
ii) Risk

(6 marks)

1.4) Briefly explain the process of risk assessment. Give three(3) examples of risk response strategies for organizations.

(6 marks)

1.5) Briefly describe three(3) key principles in designing secure information systems with human behaviour in mind.

(4 marks)

QUESTION 2

2.1) Define **Symmetric Key** cryptography.

(3 marks)

2.2) Briefly explain the **Hash Functions** in Cryptography.

(4 marks)

2.3) Describe the ***Advanced Encryption Standard (AES)*** and its advantages over ***Data Encryption Standard (DES)***.

(6 marks)

2.4) Explain three(3) management challenges associated with symmetric key cryptography.

(6 marks)

2.5) Discuss the advantages and disadvantages of **Symmentric** and **Assymmetric** key cryptography.

(6 marks)

QUESTION 3

3.1) Differentiate between ***HTTP*** and ***HTTPS*** protocols.

(3 marks)

3.2) Briefly explain the following HTTP methods.

i) POST
ii) GET
iii) PATCH

(6 marks)

3.3) Differentiate between ***SSL*** and ***TLS***. Briefly describe the following certificates in *SSL/TLS*.

i) Domain Validates(DV) Certificates
ii) Organization Validated(OV) Certificates

(5 marks)

3.4) Briefly explain the ***Network Access Control(NAC)***. Give three(3) benefits of NAC for organizations.

(5 marks)

3.5) Briefly describe **three(3)** software security best practices.

(6 marks)

QUESTION 4

4.1) Define the term ***Authentication***.

(4 marks)

4.2) Briefly explain the **password authentication**.

(4 marks)

4.3) Describe the **Hash function** for protecting the password file.

(6 marks)

4.4) What is **password salting**?

(4 marks)

4.5) Briefly explain the three(3) **Multi-Factor Authentication(MFA)** methods with examples.

(7 marks)