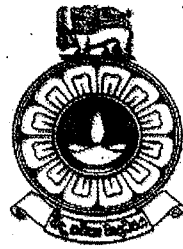


THE OPEN UNIVERSITY OF SRI LANKA
DEPARTMENT OF COMPUTER SCIENCE
BSC(IT) DEGREE PROGRAM – 2024/2025
FINAL EXAMINATION
ITU5307–CYBER SECURITY
DURATION: TWO HOUR (2 HOURS)



Date: 13.11.2025

Time: 9.30 AM – 11.30 AM

General Instructions

- 1. Read all instructions carefully before answering the questions.**
- 2. This question paper consists of 06 questions on 04 pages.**
- 3. Answer any 04 questions only. All questions carry equal marks.**
- 4. The answer for each question should commence from a new page.**
- 5. Draw fully labeled diagrams where necessary.**
- 6. Involvement in any activity that is considered an exam offense will lead to punishment.**
- 7. Use blue or black ink to answer the questions.**
- 8. Clearly state your index number in your answer script.**

Q1

Sunrise Medical Center (SMC) is a major healthcare institution with several hospitals and diagnostic centers operating across multiple cities. It uses an integrated digital healthcare platform that connects patient registration, electronic health records (EHR), diagnostic imaging systems, telemedicine applications, and billing systems. Much of SMC's infrastructure runs in a hybrid environment combining on-premises servers with third-party cloud services.

Recently, SMC experienced a severe cybersecurity incident. Attackers exploited a vulnerability in third-party remote access software used by external medical consultants. Through this entry point, the attackers gained unauthorized access to the hospital network and deployed data exfiltration malware. Over several weeks, sensitive patient information, including medical histories, prescriptions, insurance details, and contact information, was silently extracted from the network.

The breach was discovered when abnormal outbound network traffic was detected by the security operations center (SOC). However, by then, more than 150,000 patient records had already been compromised. Soon after, the stolen data appeared for sale on the dark web, and several patients began reporting phishing attempts using their stolen information.

The data breach not only caused reputational damage but also raised legal concerns under HIPAA and other data protection laws. The hospital had to suspend its telemedicine services temporarily and conduct a full forensic investigation.

- i. Who are the different types of cyber attackers targeting Sunrise Medical Center, and what are their roles in this scenario?
- ii. What security weaknesses allowed cyber-attacks to happen?
- iii. What immediate actions should Sunrise Medical Center take to mitigate the risks from this cyber-attack?
- iv. What long-term strategies should the hospital implement to prevent future breaches?

Q2

AeroTech Innovations, a global leader in aerospace and defense engineering, develops advanced satellite systems and next-generation drone technologies for government and commercial clients. The company operates multiple international research facilities and manages highly confidential defense projects involving encrypted communications and propulsion systems.

Recently, AeroTech suffered a large-scale data breach that exposed sensitive research data, encryption algorithms, and prototype blueprints. Investigations revealed that the breach was carried out through a previously unknown vulnerability in its project management software, which

attackers exploited to gain unauthorized access. The intrusion went undetected for months, allowing the attackers to quietly harvest classified data.

Further analysis indicated that the attack bore the hallmarks of a sophisticated state-sponsored cyber-espionage group, known for targeting strategic defense organizations. The threat actors used stealthy malware to establish persistence, and their success was partly aided by a systems administrator who had disabled key monitoring functions due to internal grievances. The resulting loss of intellectual property led to widespread regulatory scrutiny, project suspensions, and serious reputational harm.

- i. What type of source of cyber threat is this organized cyber-espionage operation, and what methods did the attackers use to infiltrate AeroTech Innovations?
- ii. What steps should AeroTech Innovations take to prevent future cyber-attacks and protect its sensitive military information?
- iii. How can AeroTech Innovations mitigate the risks of future cyber-attacks, and what proactive steps should be taken to prevent a potential data breach?
- iv. How can AeroTech Innovations ensure the confidentiality of its intellectual property and maintain trust with its government clients after the breach?

Q3

- i. Explain the different types of cyber countermeasures and how they help protect information systems from unauthorized access and attacks.
- ii. Discuss the various authentication methods used in cyber security and evaluate their strengths and weaknesses.
- iii. What role does cryptography play in ensuring confidentiality and integrity in digital communication?
- iv. Compare hardware-based and software-based countermeasures, highlighting their benefits and limitations in organizational environments.

Q4

- i. Define mitigation in the context of cyber security and explain its significance in minimizing potential damage after an attack.
- ii. Describe the four main mitigation strategies with appropriate examples.
- iii. How can continuous risk monitoring support an effective mitigation strategy within an enterprise network?
- iv. Discuss the relationship between mitigation planning and business continuity management in a modern organization.

Q5

- i. What are the key components of a disaster recovery plan (DRP), and how do they support post-incident recovery?
- ii. Discuss the importance of data backup and redundancy in ensuring organizational resilience after a cyber-attack.
- iii. Explain the different types of cyber disasters and their potential impact on business operations.
- iv. Evaluate the steps organizations should take to recover from a cyber attack and prevent future occurrences.

Q6

- i. Why is personal cyber security important in the digital era, and what measures can people adopt to safeguard their data?
- ii. Discuss the significance of strong passwords and multi-factor authentication (MFA) in protecting personal accounts.
- iii. How can mobile device security practices prevent unauthorized access to sensitive information?
- iv. Explain how public Wi-Fi usage can pose cyber risks and suggest methods to stay secure while using it.

****All Rights Reserved****