ourdiu.com | Shared by Mehedi Hasan Jeon 2.4222E+14

Daffodil International University

Faculty of Science & Information Technology

Department of Computer Science & Engineering

Final Semester Examination, Summer 2025

Course Code: CSE423, Course Title: Information Security

Level: 3 Term: 2, Batch: 63

Time: 2 Hrs **Marks: 40**

Answer ALL Questions

[The figures in the right margin indicate the full marks and corresponding course outcomes. All portions of each question must be answered sequentially.]

1.	A multinational tech company recently experienced a ransomware attack that encrypted internal files and client data. In response, the company deployed honeypots to track malicious activity and implemented blockchain technology to secure transaction records and ensure data integrity. Although the attack was contained quickly by the incident response team, the breach revealed weaknesses in the company's risk management strategy, prompting a reassessment of its security protocols.			**CO1**
	a)	**Explain** the differences between security risk management and incident management, as well as risk appetite and risk tolerance, in the context of these challenges.	**[5]**	
	b)	**Apply** your understanding to explain how different types of honeypots and blockchain's characteristics (such as immutability, decentralization, and transparency) can improve the company's security strategy. Additionally **identify** the role and impact of Bitcoin and Ethereum, with a focus on smart contracts, in terms of their potential benefits for the company's security approach.	**[8+2]**	
2.	University IT has assigned students to assess the risks of five critical online systems: Library Management System, Examination Portal, Course Registration System, Staff Management Portal, and Online Payment Gateway. Risk levels vary by system based on attack likelihood and impact. For example, the Library Management System is rarely targeted but would have a severe impact if compromised, while the Examination Portal is frequently targeted and would cause considerable disruption. The Course Registration System is occasionally threatened with moderate impact, the Staff Management Portal is rarely attacked but would have serious consequences, and the Online Payment Gateway is frequently attacked, causing severe financial harm.			
	a)	Based on the provided data, **analyze** the risk level for each asset to calculate the overall risk rating.	**[5]**	**CO2**
	b)	To mitigate the risk, the university's IT department has secured its critical systems. Their antivirus software analyzes program and file code behavior to detect malware, including unknown threats not present in signature databases. The university's firewall filters incoming traffic through a proxy to hide remote users' identities and prevent direct attacks. **Analyze** the antivirus and firewall used by the university to identify the types being used and explain their working procedures.	**[2+3]**	

ourdiu.com | Shared by Mehedi Hasan Jeon 2.4222E+14

	c)	Despite existing security, the university faces network attacks and wants to strengthen communication using through encryption algorithms RSA and ElGamal. Compare between the two algorithms considering the strengths and weaknesses of each to find the most suitable one. Additionally, **analyze** how the university can make the system quantum safe suggesting four alternative algorithms.	**[2+3]**	
3.	a)	*ByteWave Technologies* is a SaaS company that offers AI-powered document processing for healthcare, finance, and legal clients. It uses both open-source software and machine learning models trained on user-uploaded data. The company stores sensitive client information on cloud platforms and recently began expanding to the European market. **Inspect** the significance of compliance from the perspective of the company. Also **examine** the relevance of some common frameworks and regulations known to you for that company.	**[5]**	**CO**
	b)	**Demonstrate** the legal consequences outlined in Sections 19 and 32 of the Digital Security Act 2023 for individuals who commit digital system damage, or hacking and how these provisions help mitigate cybercrimes	**[5]**	

ourdiu.com