Daffodil International University

Faculty of Science & Information Technology
Department of Computing and Information System
Final Examination, Summer-2026
Course Code: CIS311, Course Title: Network Security and Cryptography
Level: 3 Term: 1

Exam Duration: 2 Hours **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.]

			[Mark]	CO
1.		**Greenfield International University (GIU)** is a private university in Bangladesh, established in 2008. It has a main campus in Dhaka and one branch campus in Chittagong. The university has approximately 15,000 students and 800 faculty members. GIU provides various online services including a Student Portal, Online Examination System, Library Management System, and Faculty Research Database. The university recently launched a Smart Campus Network and the main server is located at the Dhaka campus with IP address **192.168.10.5**. Recently, GIU experienced the following security incidents: • A student hacked into the examination system and changed his grades. • Login credentials of several faculty members were stolen. • The student portal was down for 2 days after a Denial-of-Service (DoS) attack. • A third-party attacker intercepted emails between faculty members containing unpublished research data. The university's board has decided to fully upgrade the security of GIU's network. The IT security team must now design and implement a proper security system to protect all university assets and data.		
	a)	The recent security incidents at GIU clearly violated the core principles of information security. Define each of the three objectives of the CIA Triad as described by NIST (FIPS 199).	[3]	CO1
	b)	GIU's IT team decided to protect all student exam data and research files using AES-192 encryption. Describe the complete working steps of the AES algorithm.	[7]	
	c)	To prevent email interception and protect faculty research communications, GIU adopts RSA encryption. Demonstrate the encryption and decryption using two prime numbers p = 3 and q = 7, public key exponent e = 5 and the plaintext message M = 2.	[5]	
2.	a)	GIU's IT team recommends setting up a PKI to manage digital certificates for all staff and students. List the main components of a PKI. Describe the role of each component and explain how they would function within GIU's network to authenticate users.	[5]	CO2

	b)	The Student Portal must use SSL/TLS to protect student logins and online exam submissions. I. Differentiate between an SSL Session and an SSL Connection. II. Describe the SSL Handshake process and explain why it is important for securing the connection between a student's browser and GIU's portal server.	[2+4]	
3.	a)	The security team performs a Penetration Test on GIU's examination system and student portal. I. Describe what a penetration test is. II. Draw the TCP Three-Way Handshake diagram between the scanner and GIU's system port and explain why this scan is easily detected.	[1+4]	CO3
	b)	To fix the weak login system, GIU must redesign how users authenticate on the network. I. Explain Multi-Factor Authentication (MFA) and why it is more secure than a simple password. II. Recommend an MFA approach for this case: "A student logging into the Online Examination System".	[2+2]	
4.	a)	The table below presents a small portion of the ACL configured on GIU's firewall. Using these rules, determine whether each network request is allowed or blocked.	[2]	CO3

In a single word

Rule	Source IP	Source Port	Dest. IP	Dest. Port	Action	Comment
1	*	*	10.10.1.20	443	Allow	Allow HTTPS access to the Student Portal server
2	192.168.20.50	*	*	*	Block	Block all traffic from the compromised student computer
3	*	*	10.10.1.30	22	Allow	Allow SSH access to the IT Management Server

I. What happens if 192.168.20.50 sends an HTTPS request (port 443) to 10.10.1.20 (Student Portal Server)?
II. What happens if 192.168.10.25 (Faculty PC) sends an SSH request (port 22) to 10.10.1.30 (IT Management Server)?

	b)	The university's IT department has assigned private IP addresses to all internal devices across the two campuses. However, GIU only has one single public IP address provided by its Internet Service Provider (ISP) for all outgoing internet traffic. To manage this situation, GIU's network router uses Network Address Translation (NAT). Describe how NAT operation works in GIU's campus network.	[3]	