ourdiu.com | Shared by MD. RIDWAN AHMED

Daffodil International University

Faculty of Science & Information Technology

Department of Software Engineering

Midterm Examination, Fall 2026

Course Code: SE332; Course Title: Information System Security

Sections & Teachers: 42 & (A,B,C,D) IAT, (E,F,G)UKD, (H)RI,(I)AHZ, (J)AHR

Time: 1 Hour 30 Mins **Marks: 25**

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.	During a discussion about a recent university security incident, Rafi explained that a cybersecurity researcher had discovered an expired password-reset link that could still be reused. The researcher tested the weakness on an authorized account and reported the issue. However, the IT team did not address the reported weakness or conduct additional security testing. A few days later, another individual exploited the same weakness to secretly modify students' grades. The incident remained undetected for several days because the system lacked effective security monitoring. After hearing this, Sami argued that the researcher was a cracker because they had tested the weakness, while the individual who modified the grades was a hacker because they demonstrated technical skill. Sami further claimed that the password-reset flaw was initially a threat and only became a vulnerability after the grades were changed.			**CLO-1** ***Level-3*** ***8 marks***
	a)	Critically evaluate Sami's statements and **determine** whether his interpretations are correct or incorrect. **Illustrate** your evaluation by identifying and explaining the **vulnerability, threat, hacker, and cracker** in the given scenario.	**[Marks-4]**	
	b)	**Identify** the security **shortcomings** in the scenario, and suggest preventive measures based on the relevant SSDLC phases.	**[Marks-4]**	
2.	***a)***	A university has developed a web-based Student Management System where students can view their academic records, course registrations, and payment information. During a security assessment, it was discovered that a student could modify the student ID in the URL to access another student's confidential records. Furthermore, by manipulating certain HTTP requests, the student could change other students' grades and execute administrative operations without having the necessary privileges. **Determine** the security vulnerabilities that may have enabled these activities and propose appropriate strategies to prevent such attacks.	**[Marks-5]**	**CLO-1** ***Level 3*** ***8 marks***

ourdiu.com | Shared by MD. RIDWAN AHMED

	b)	Students in a university laboratory exchange applications using USB drives and shared folders. Technicians discover that malicious code has attached itself to several executable files and spreads whenever those files are executed. A second malicious program independently scans the laboratory network and copies itself to other computers without requiring users to open infected files. Meanwhile, several computers begin receiving instructions from an external server and simultaneously flood a public website with traffic. **Identify** the distinct types of malware indicated by the scenario. Explain the reasoning behind your conclusions. Propose one countermeasures for each identified malware type.	[Marks-3]	
3.	a)	A cybersecurity researcher discovers a secret message encrypted using a three-stage cascading encryption system based on the given 24-character index table (indices 0–23) in appendix A. In the first stage, decrypt the Caesar ciphertext **π ♥ + Ω C** using a Caesar **shift of 7**. In the second stage, use the five-character plaintext obtained from the Caesar decryption as the OTP key to decrypt the ciphertext **θ @ ♣ # α** . In the final stage, take the first four characters of the recovered OTP plaintext, convert them into numerical indices, group them into pairs, and decrypt them using a Hill cipher with key matrix K: $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ **Determine** the final four-character plaintext.	[Marks-2+ 2.5+2.5]	**CLO-2** ***Level-3*** ***9 marks***
	b)	A cybersecurity analyst intercepts the plaintext **UREVEM** encrypted using the Playfair cipher with the keyword **SECURITY**. Decrypt the ciphertext to recover the original plaintext. Show the Playfair matrix construction, ciphertext pair formation, and the decryption steps for each pair.	[Marks-2]	

Appendix A:

Index	*Character*	*Index*	*Character*	*Index*	*Character*
0	A	8	α	16	★
1	B	9	β	17	♠
2	C	10	γ	18	♣
3	D	11	δ	19	♥
4	E	12	θ	20	♦
5	F	13	λ	21	+
6	G	14	π	22	#
7	H	15	Ω	23	@