Daffodil International University

Faculty of Science & Information Technology

Department of Software Engineering

Final Examination, Spring 2026

Course Code: SE332; Course Title: Information System Security

Sections & Teachers: 41 & (A,K) RI, (B)AE, (C,D,E,F)IAT,(G,H,I,J)MBH, (L,M)HT, (N)RBG

Time: 2:00 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.

1	0	0	1
1	0	1	1
0	1	1	0
0	1	1	1
1	0	0	0
1	1	0	0
0	1	1	0
1	0	1	1

Appendix A: 32 bit L_{i-1}

(Value Given)

1	0	0	1
1	0	1	1
1	1	1	0
0	1	1	1
0	0	0	0
0	1	0	0
0	0	1	0
1	0	1	1

Appendix B: 32 bit R_{i-1}

(Value Given)

a)	**Evaluate** how the principles of confusion and diffusion address the weaknesses of classical stream ciphers. **Justify** your answer by illustrating the Fiestal network concept.	[Marks-6]	CLO-3 *Level-5*
b)	In the DES Expansion Permutation, each 4-bit block of the 32-bit input (**Appendix B**) is expanded into a 6-bit block. If the **third** 4-bit input block is 1110 and if you are asked to expand this 4 bit input block to 6 bit input block, then how expansion logic will help you. To **justify** this, calculate the 6-bit output for this 3rd block using the expansion logic.	[Marks-5]	
c)	Suppose you are asked to calculate the value of S-box. Determine why DES expands the 32-bit right half to 48 bits before the XOR operation. Figure out the issues or obstacles that would occur in the S-box substitution if this step were skipped.	[Marks-4]	

		And also if you are asked to calculate the value of L_i, identify the logical operation used to calculate the value of L_i and explain how **Appendix B** helps you determine the output.		
2.	*a)*	**Explain** how the number of rounds in Advanced Encryption Standard varies with key size. **Justify** your answer with a diagram.	**[Marks-5]**	**CLO-3** *Level-5*
	b)	**To explain** the process of AES round key generation, determine how the Rcon table contributes to generating the Round 2 (R2) key from Round 1 (R1), **justifying** your answer with the appropriate steps.	**[Marks-5]**	
	c)	An attacker is attempting a brute-force attack on two encrypted systems: System A uses AES-128 , System B uses AES-256 The attacker has a total budget of $2,000,000, where each custom ASIC costs $200 (including all operational overhead). Each ASIC can test 2×10^9 keys per second, and all ASICs operate in parallel. Using appropriate calculations and reasoning: i) **Assess** the feasibility of successfully brute-forcing each system. ii) **Compare and evaluate** the computational effort required for AES-128 and AES-256.	**[Marks-5]**	
3.		A secure communication system named DataTrust uses RSA for encryption and Digital Signature Algorithm (DSA) for authentication. The system ensures that all sensitive messages exchanged between users remain confidential and tamper-proof. Suppose a user, Neerai, wants to send a secure message to a server. The system performs the following: • RSA is used to generate public and private keys using two prime numbers. • Neerai signs the message using a digital signature scheme before sending it. • The receiver verifies the signature using Neerai's public key. • If the message is altered during transmission, the system should detect it. Answer all the questions with proper justification.		
	a)	Using the prime numbers p = 13 and q = 19, and a public key e = 5, determine the private key and verify the correctness of the key pair using a message M = 4.	**[Marks-05]**	**CLO-4** *Level-4*
	b)	Explain how a digital signature is generated and verified using RSA in this system. Clearly describe: • The signing process • The verification process • How authentication and integrity are ensured	**[Marks-05]**	