# Daffodil International University
## Department of Software Engineering
## Faculty of Science & Information Technology
**MID Examination, Fall 2025**

**Course Code: SE332; Course Title: Information System Security**

**Sections & Teachers: (MBH-A, B), (AE-C), (TM-D, E), (AE-F, G, H), (DDK-I)**

**Time: 1 Hour 30 Minutes** **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. | a) | At "MediSys Health Portal," a web-based system used by several hospitals to store and retrieve patient records, the IT security team recently updated the system's access control module. After the update, some unusual login attempts went unnoticed for several weeks because the automated alert system was not working properly. As a result, this delay caused a minor data breach attempt.<br><br>Additionally, the hospital's legal team later discovered that certain archived patient records from five years ago were missing. These records were needed for a compliance audit. When the technical team checked the backup servers, they found that the data was not properly synchronized with newer storage hardware introduced last year, leading to partial data loss.<br><br>**Demonstrate** why the hospital faced issues in detecting unauthorized access and retrieving old patient records, and explain how these issues can be effectively mitigated through improved operational security practices and system maintenance. | [Marks-5] | CLO-1<br>*Level-3* |
| | b) | A small startup, TechNova Solutions, recently experienced a security incident. Employees downloaded what appeared to be a "free antivirus update" and a "system optimization tool" from an email and unverified websites. After installation, some files went missing, certain programs stopped working, and confidential company data seemed to be accessed remotely without authorization.<br><br>**Analyze** what might have happened to the company's systems based on this scenario, and explain the type of malware involved, how it could have entered the system, and why it was able to cause harm while appearing safe to users. | [Marks-5] | |

| | | | | |
|---|---|---|---|---|
| 2. | | Imagine you're developing a web application that has a user registration form. The form collects user inputs such as username, age, date of birth, email, and password. To keep the system secure and prevent attacks like SQL injection, cross-site scripting (XSS), and other injection attacks, you figured out that you have to implement the process of input validation.<br><br>So, if you want to get a secure system against these attacks, what initiative will you take? **Illustrate** the process. | **[Marks-6]** | **CLO-1** *Level-3* |
| 3. | a) | **Apply** the Decryption process of "One Time Pad" where you have given a key value **"INFORMATION SYSTEM SECURITY"** and a cipher text **"MSIGQCUBRAZVHIBJE"**. Start the value of the alphabet from 1 (i.e. A=1, B=2, C=3, ....., Z=26). | **[Marks-3]** | **CLO-2** *Level-3* |
| | b) | Currently you have given a shared key of Hill Cipher (given below) and a message "GOOD". To select the right process, follow the answer of question **3(a)** as an ***Instruction***. Answer to question **3 (a)** will help you as a clue to **discover** what kind of value you should generate.<br><br>Encryption Key= $\begin{bmatrix} 3 & 2 \\ 3 & 5 \end{bmatrix}$<br><br>Start the value of the alphabet from 0 (i.e. A=0, B=1, C=2, ....., Z=25). | **[Marks-3]** | |
| | c) | **Apply the encryption** technique of Play Fair algorithm to calculate the value of cipher text using the given plain text as **"GENEREETED THE VALUE OF PLAIN TEXT"** and consider the answer of Question 3 (b) as a key value here. | **[Marks-3]** | |