diuqbank.com | Shared by Khabbab HS

Daffodil International University

Faculty of Science & Information Technology

Department of Information Technology & Management

Final Examination, Summer 2025

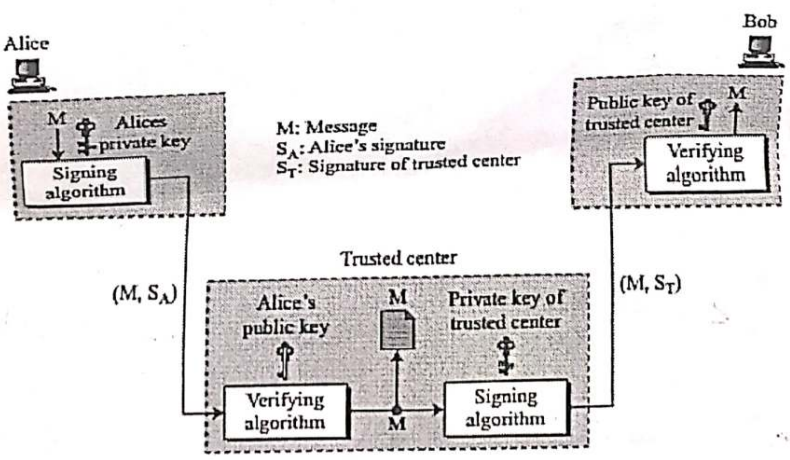
Course Code: ITM 322; Course Title: Software and Web Security

Sections & Teachers: A (AR)

Time: 2:00 Hours **Marks: 40**

Answer ALL Questions

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

1.	a)	**Define** Honeypot? **Outline** different types of database security controls with brief description?	[Marks-4]	CO-1 Level-1
	b)	You are given a plaintext and a keyword. **Perform** encryption using the *"Autokey Cipher"* and find the final ciphertext. **Plaintext:** DAFFODILITM **Key:** 9 (As you are from 9th batch)	[Marks-4]	CO-2 Level-3
2.	a)	***State*** the term digital signature. **Demonstrate** how blockchain works with a diagram with brief description.	[Marks-4]	CO-4 Level-3
	b)	You are given plaintext and a keyword. **Perform** encryption using the *"Playfair Cipher"* method and find the final ciphertext. **Plaintext:** YELLOWBUDS **Keyword:** DAFFODIL	[Marks-4]	CO-2 Level-3
3.	a)	**Explain** any five common web application vulnerabilities caused by bad design with example for each.	[Marks-4]	CO-1 Level-2
	b)	 **Analyze** the working process of nonrepudiation using a trusted third party based on the provided diagram.	[Marks-4]	CO-4 Level-4

diuqbank.com | Shared by Khabbab HS

4. (a) **Illustrate** the working principle of CMAC (also known as CBCMAC) with a proper diagram. [Marks-4] CO-3 Level-4

b) A website has a login form where users enter their username and password. The server processes this input using an insecure SQL query:

```
$email = $_POST['email'];
$pass = $_POST['pass'];
$sql = "SELECT * FROM accounts WHERE
email = '$email' AND pass = '$pass'";
$result = mysqli_query($conn, $sql);
```

[Marks-4] CO-1 Level-2

Interpret how SQL Injection can occur in this login system and **explain** how an attacker could exploit it to bypass authentication using malicious input.

5. a) ***Summarize*** how Cross-Site Request Forgery (CSRF) attacks are executed in web applications and **present** a few effective prevention techniques to mitigate such attacks. [Marks-4] CO-1 Level-2

(b) **Formulate** example for each -

- Insecure Direct Object Reference and
- Insecure Cryptographic Storage

with brief justification. [Marks-4] CO-1 Level-5