Amrita Vishwa Vidyapeetham
Amrita School of Computing
Department of Computer Science and Engineering
23CSE313 - FOUNDATIONS OF CYBER SECURITY

LAB EVALUATION 1

Objective

Assessing student's understanding and practical implementation of core security concepts that includes the topics covered - **Authentication, Authorization (Access Control), Encryption, Hashing and Encoding** through a **real-world application**. **Each student** must design and implement an application where all security concepts are integrated cohesively.

Application Requirement

- Student must first **select a real-world application** such as secure file sharing, e-voting system, hospital record system, exam portal, banking module, etc. (Preferably reuse the application developed as part of UID course along backend and database included)
- The selected application must **implement all the following security components**.
- The user Registration and Login processes must follow NIST SP 800-63-2 E-Authentication Architecture Model.

Note to students

- No two applications should be the same.
- Applications must be original, realistic, and strong in security design.

Evaluation Components & Marks Breakdown

Laboratory Evaluation – Marks Breakdown

S. No.	Evaluation Component	Sub-Component	Description / Expectation	Mark	Total
1	**Authentication**	Single-Factor Authentication	Implementation using password / PIN / username-based login	**1.5**	**3m**
		Multi-Factor Authentication	Implementation using at least two factors (e.g., password + OTP, password + email code, password + biometric simulation)	**1.5**	
2	**Authorization - Access Control**	Access Control Model	Implement Access Control Matrix or Access Control List (ACL) with minimum 3 subjects and 3 objects		

		Policy Definition & Justification	Clearly define and justify access rights (who can access what and why)	**1.5**	**3m**
		Implementation of Access Control	Enforce access permissions programmatically in the application	**1.5**	
3	**Encryption**	Key Exchange Mechanism	Demonstrate secure key generation or key exchange method	**1.5**	**3m**
		Encryption & Decryption	Implement secure encryption and decryption (e.g., AES, RSA, hybrid approach)	**1.5**	
4	**Hashing & Digital Signature**	Hashing with Salt	Secure storage of passwords/data using hashing along with salt	**1.5**	**3m**
		Digital Signature using Hash	Demonstrate data integrity and authenticity using hash-based digital signatures	**1.5**	
5	**Encoding Techniques**	Encoding & Decoding Implementation	Implement encoding and decoding using one technique (Base64 / QR Code / Barcode / CodeChef-relevant encoding)	**1**	**3m**
		Security Levels & Risks (Theory)		**1**	
		Possible Attacks (Theory)		**1**	
6.a	**Viva**	Oral Examination	Assess conceptual clarity, security reasoning, design choices, and awareness of attacks and countermeasures, etc….	**2**	
6.b	**Class Participation / Continuous Assessment**	Participation / Assignments	Based on weekly assignments, lab progress, class notes, or discussions	**3**	
7			**Complete Viva**	**5**	
NOTE: Component 6 (Viva +participation) or 7 (only viva) - any one can be considered. i.e.,(2m+3m) or (5m)					**5m**
TOTAL					**20m**