MIT ACADEMY OF ENGINEERING

Department of Computer Engineering

Cryptography and Information Security

Subject code: 2304324L

Guidelines and Rubrics for CIS Practical Exam

Subject: Cryptography & Information Security

Exam Type: Project Demonstration + Presentation + Viva

Date: 29th November

Venue: H302

Reporting Time: 9:00 AM (Sharp)

Team Size: 4–5 Students

Total Marks: 30

All the students are informed to strictly follow the CIS Practical- project examination guidelines. Exam is scheduled on 29th November at 9:00 AM in H302.

1. Each group must design and implement a mini-project related to **Cryptography, Network Security, or Information Security**. The project must involve:

- A **working implementation/demo**
- Use of **security concepts from the syllabus**
- A **presentation** summarizing the work
- **Viva** to evaluate individual contribution

2. T**eam Guidelines:**

- You are not allowed to change/ add team members on the day of exam. Team detail mentioned in the shared google sheet is considered as final team.
- Every member must present for at least 1–2 minutes.
- Each member must answer at least 1 viva question.
- Marks will be **deducted if contribution appears uneven**.

3. **Exam Flow:**

We will follow google sheet sequence for the evaluation. ie. the first team from the sheet will come first for the evaluation. Unavailability of the team, on the said time will be treated as ABSENT. No excuses will be entertained for change in sequence of the team.

4. Rubrics: 30 Marks

Category	**Excellent**	**Good**	**Average**	**Below Average**	**Poor**	**Marks**
1. Problem Definition & Relevance (5 Marks)	Clear, well-defined problem; strong relevance to cryptography/ security; innovative; measurable objectives. **(5 marks)**	Clear problem; relevance explained; some novelty. **(4 marks)**	Basic statement; limited justification. **(3 marks)**	Vague scope; weak relevance. **(2 marks)**	No clarity or copied topic. **(0–1 marks)**	**/5**
2. Technical Design & Architecture (5 Marks)	Detailed architecture; correct crypto/security selection; proper diagrams;	Good design; clear diagrams; correct concept	Basic design with limited depth. **(3 marks)**	Minimal diagrams; weak justifica	Incorrect or missing architecture. **(0–1 marks)**	**/5**

	threat model included; high depth. **(5 marks)**	usage. **(4 marks)**		tion. **(2 marks)**		
3. Implementation Quality & Working Output (10 Marks)	Fully working project; stable output; real crypto/security implementation; technically strong; innovative. **(9–10 marks)**	Mostly working; minor issues; correct security concepts. **(7–8 marks)**	Partially working; basic output. **(5–6 marks)**	Incomplete; mostly theoretical. **(3–4 marks)**	No working output or copied code. **(0–2 marks)**	**/10**
4. Presentation & Communication (5 Marks)	Clear, confident; strong explanation of concepts; clean slides; smooth demo. **(5 marks)**	Good clarity; structured flow; small gaps. **(4 marks)**	Basic presentation; lacks clarity in parts. **(3 marks)**	Poor slides; weak delivery. **(2 marks)**	No preparation; unable to explain. **(0–1 marks)**	**/5**
5. Viva + Individual Contribution (5 Marks)	All members answer confidently; deep understanding; clear ownership of work. **(5 marks)**	Most answer well; fair contribution. **(4 marks)**	Some understanding; uneven contributions. **(3 marks)**	Weak answers; 1–2 members dominate. **(2 marks)**	No understanding; no visible contribution. **(0–1 marks)**	**/5**