	Universitas Negeri Surabaya Faculty of Engineering, Electrical Engineering Undergraduate Study Program			Document Code

SEMESTER LEARNING PLAN

Courses	CODE	Course Family	Credit Weight			SEMESTER	Compilation Date
Cryptography	2020102067		T=2	P=0	ECTS=3.18	7	July 18, 2024

AUTHORIZATION	SP Developer	Course Cluster Coordinator	Study Program Coordinator
	....	....	Dr. Lusia Rakhmawati, S.T., M.T.

Learning model	Case Studies

Program Learning Outcomes (PLO)	PLO study program that is charged to the course
	Program Objectives (PO)
	PLO-PO Matrix
	P.O
	PO Matrix at the end of each learning stage (Sub-PO)

P.O	Week															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Short Course Description	This course discusses the concepts of the history of cryptography, modular arithmetic, modular exponentiation, stream ciphers, introduction to public key cryptography, digital signatures, and message authentication codes (Macs). This course is presented in theoretical form

References	Main :	
	1.	1.cristof pear" Understanding criptograpy" springer 2.wiliam stallings " criptography and network security
	Supporters:	

Supporting lecturer	Dr. Farid Baskoro, S.T., M.T. Arif Widodo, S.T., M.Sc.

Week-	Final abilities of each learning stage (Sub-PO)	Evaluation		Help Learning, Learning methods, Student Assignments, [Estimated time]		Learning materials [References]	Assessment Weight (%)
		Indicator	Criteria & Form	Offline (offline)	Online (online)		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)

1	Students are able to know the history of cryptography	students know the Enigma machine and its benefits		discussion, lecture and question and answer 2 X 50			0%
2	1. Students are able to understand symmetric crytography2. Students know cryptoanalysis 3. Students know modular arithmetic	1. Students understand the basics of symmetric cryptography and simple symmetric encryption2. Students know modular arithmetic 3. Students know ring integer 4. Students know the shift cipher		discussion, lecture and question and answer 2 X 50			0%
3	1. Students are able to understand symmetric crytography2. Students know cryptoanalysis 3. Students know modular arithmetic	1. Students understand the basics of symmetric cryptography and simple symmetric encryption2. Students know modular arithmetic 3. Students know ring integer 4. Students know the shift cipher		discussion, lecture and question and answer 2 X 50			0%
4	Students understand stream chippers	1. Understanding stream ciphers Vs Block ciphers2. Students are able to understand encryption and description via stream ciphers3. Students know random number unbreakable stream ciphers4. Students know the shift register through stream ciphers		discussion, lecture and question and answer 2 X 50			0%
5	Students understand stream chippers	1. Understanding stream ciphers Vs Block ciphers2. Students are able to understand encryption and description via stream ciphers3. Students know random number unbreakable stream ciphers4. Students know the shift register through stream ciphers		discussion, lecture and question and answer 2 X 50			0%
6							0%

7							0%
8							0%
9							0%
10							0%
11							0%
12							0%
13							0%
14							0%
15							0%
16							0%

Evaluation Percentage Recap: Case Study

No	Evaluation	Percentage
		0%

Notes

1. **Learning Outcomes of Study Program Graduates (PLO - Study Program)** are the abilities possessed by each Study Program graduate which are the internalization of attitudes, mastery of knowledge and skills according to the level of their study program obtained through the learning process.
2. **The PLO imposed on courses** are several learning outcomes of study program graduates (CPL-Study Program) which are used for the formation/development of a course consisting of aspects of attitude, general skills, special skills and knowledge.
3. **Program Objectives (PO)** are abilities that are specifically described from the PLO assigned to a course, and are specific to the study material or learning materials for that course.
4. **Subject Sub-PO (Sub-PO)** is a capability that is specifically described from the PO that can be measured or observed and is the final ability that is planned at each learning stage, and is specific to the learning material of the course.
5. **Indicators for assessing** ability in the process and student learning outcomes are specific and measurable statements that identify the ability or performance of student learning outcomes accompanied by evidence.
6. **Assessment Criteria** are benchmarks used as a measure or measure of learning achievement in assessments based on predetermined indicators. Assessment criteria are guidelines for assessors so that assessments are consistent and unbiased. Criteria can be quantitative or qualitative.
7. **Forms of assessment:** test and non-test.
8. **Forms of learning:** Lecture, Response, Tutorial, Seminar or equivalent, Practicum, Studio Practice, Workshop Practice, Field Practice, Research, Community Service and/or other equivalent forms of learning.
9. **Learning Methods:** Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, and other equivalent methods.
10. **Learning materials** are details or descriptions of study materials which can be presented in the form of several main points and sub-topics.
11. **The assessment weight** is the percentage of assessment of each sub-PO achievement whose size is proportional to the level of difficulty of achieving that sub-PO, and the total is 100%.
12. TM=Face to face, PT=Structured assignments, BM=Independent study.