	Universitas Negeri Surabaya Faculty of Mathematics and Natural Sciences Undergraduate Mathematics Study Program	Document Code

SEMESTER LEARNING PLAN

Courses	CODE	Course Family	Credit Weight			SEMESTER	Compilation Date
Introduction to Cryptography	4420102097	Algebra	T=2	P=0	ECTS=3.18	5	April 26, 2023

AUTHORIZATION	SP Developer	Course Cluster Coordinator	Study Program Coordinator
	R. Sulaiman	.....	Prof. Dr. Raden Sulaiman, M.Si.

Learning model	**Project Based Learning**

Program Learning Outcomes (PLO)

PLO study program that is charged to the course

Program Objectives (PO)

PO - 1	Responsible for completing tasks within the specified time
PO - 2	Applying number concepts in problem solving
PO - 3	Convey ideas in writing and orally regarding innovations in cipher preparation
PO - 4	Understand mathematical concepts related to number theory

PLO-PO Matrix

P.O
PO-1
PO-2
PO-3
PO-4

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
PO-1																
PO-2																
PO-3																
PO-4																

Short Course Description

This course examines the history and basic concepts of cryptography, symmetric and asymmetric crypto systems. The symmetric crypto systems discussed are: Caesar chipper, Monoalphabetic, Vigenere, One Time Pad, Palyfair, ADFGVX, and Affine cipher. Meanwhile, the asymmetric crypto system discussed is RSA.

References

Main :

1. Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag
2. Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag
3. Paul Garret. 2001. An introduction to Cryptology. New York: Printice Hall
4. Simon Singh. 2004. Code Book

	Supporters:	
Supporting lecturer	Prof. Dr. Raden Sulaiman, M.Si.	

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	Understand mathematical concepts related to number theory	• Write down the meaning of cryptosystem • Carry out encryption and decryption	**Form of Assessment** : Participatory Activities		Online, students carry out simple encryption and decryption		10%
2	1.• Determine the cipher text 2.• Carry out decryption with the Caesar wheel	1.• Determine the cipher text 2.• Carry out decryption with the Caesar wheel			Online, Create a Caesar Wheel and use it; Using software	**Material:** Caesar Cipher **Library:**	10%
3	Understanding mathematics related to the divisibility of numbers	1.• Decrypt English text messages 2.• Decrypt Indonesian messages			Learning is carried out online; Students conducted a survey on the use of alphabets in English and Indonesian texts	**Material:** Mono Alphabetic **Reader:** *Simon Singh. 2004. Code Book*	0%
4	Applying number theory concepts in decrypting messages	• Decrypt messages using: Caesar cipher and Mono Alphabetic			Learning is carried out online; Practice "Crack code" with Caesar Ciper and Mono Alphabetic	**Material:** Caesar and Mono Alphabetic **Literature:** *Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag*	0%
5	Applying the concept of number theory in encrypting and decrypting messages	1.• Encrypt messages with Vigenere cipher 2.Encrypt messages with One Time Pad cipher			Learning is done online. Students carry out encryption and decryption.	**Materials:** 3. Vigenere 4. One Time Pad **Reader:** *Simon Singh. 2004. Code Book*	0%
6	Applying the concept of number theory in encrypting and decrypting messages	1.• Encrypt messages with Vigenere cipher 2.Encrypt messages with One Time Pad cipher	**Form of Assessment** : Participatory Activities		Learning is carried out online. Students carry out encryption and decryption	**Material:** One Time Pad **Reader:** *Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag*	0%

7	Applying the concept of number theory in encrypting and decrypting messages	1.• Decrypt messages using Caesar Cipher 2.Decrypt messages using Mono Alphabetic 3.Decrypt messages using Vigenere and One Time pad	**Form of Assessment** : Participatory Activities		Learning is carried out online. Discuss and practice “Crack code” with Caesar Ciper, Mono Alphabetic, Vigenere and One Time pad	**Material:** Caesar Cipher, Mono Alphabetic, Vigenere and One Time pad **Library:**	0%
8					UTS		0%
9	Able to communicate ideas orally	• Encrypt and decrypt messages with ADFGVX cipher	**Form of Assessment** : Participatory Activities		Learning is carried out online. Discuss ADFGVX cipher	**Material:** ADFGVX cipher **Reader:** *Paul Garret. 2001. An introduction to Cryptology. New York: Printice Hall*	0%
10	Work together in groups to share new ideas and ideas for making chips		**Form of Assessment** : Participatory Activities		Online learning. Discuss: • ECB mode • CBC mode • CFB mode • OFB mode	**Material:** • ECB mode • CBC mode • CFB mode • OFB mode **References:** *Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag*	0%
11	Work together in groups to share new ideas and ideas for making chips	Able to develop new ciphers	**Form of Assessment** : Participatory Activities		Online learning. Discuss: • ECB mode • CBC mode • CFB mode • OFB mode	**Material:** • ECB mode • CBC mode • CFB mode • OFB mode **References:** *Hans Delfs and Helmut Knebl. 2007. Introduction to Cryptography. New York: Springer-Verlag*	0%
12	Share thoughts and ideas in groups	Able to develop new ciphers	**Forms of Assessment** : Participatory Activities, Project Results Assessment / Product Assessment		discuss as a group the project task, developing a new cipher based on several ciphers that are already known to students. This project task was completed within 3 weeks (weeks 10-12). Weeks 13-15 Students take turns presenting the results of their projects.	**Material:** New cipher construction **Reference:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%
13	Discuss discussions and communicate in groups	Able to develop new ciphers	**Forms of Assessment** : Participatory Activities, Project Results Assessment / Product Assessment		discuss as a group the project task, developing a new cipher based on several ciphers that are already known to students. This project task was completed within 3 weeks (weeks 10-12). Weeks 13-15 Students take turns presenting the results of their projects.	**Material:** New cipher construction **Reference:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%

14	Discuss in developing new ciphers	Able to communicate thoughts and ideas	**Forms of Assessment** : Participatory Activities, Project Results Assessment / Product Assessment, Practices / Performance		Online, students present the results of projects to develop new ciphers based on several ciphers that students already know.	**Material:** Presentation **Bibliography:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%
15	Communicate in writing and orally about new ciphers	Able to communicate thoughts and ideas	**Forms of Assessment** : Participatory Activities, Project Results Assessment / Product Assessment		Online, students present the results of projects to develop new ciphers based on several ciphers that students already know.	**Material:** Presentation **Bibliography:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%
16		Reporting the results of project work	**Forms of Assessment** : Participatory Activities, Project Results Assessment / Product Assessment		Finalization of project report results	**Material:** Preparation of report **Bibliography:** *Johannes A. Buchmann. 2001. Introduction to Cryptography. New York: Springer-Verlag*	0%

Evaluation Percentage Recap: Project Based Learning

No	Evaluation	Percentage
1.	Participatory Activities	10%
		10%

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** abilities in the process and student learning outcomes are specific and measurable statements that identify the abilities 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.