MODULE HANDBOOK
CRYPTOGRAPHY

BACHELOR DEGREE PROGRAM
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE AND DATA ANALYTICS

INSTITUT TEKNOLOGI SEPULUH NOPEMBER

MODULE HANDBOOK
PROBABILITY AND STATISTICS

Module name	**Cryptography**
Module level	Bachelor
Code	KM184830
Course (if applicable)	Cryptography
Semester	Spring (Genap)
Person responsible for the module	Dr. Darmaji, S.Si, M.T
Lecturer	Dr. Darmaji, S.Si, M.T
Language	Bahasa Indonesia and English
Relation to curriculum	Bachelor degree program, **elective**, 8th semester.
Type of teaching, contact hours	Lectures, <60 students Tuesdays, 11.00-12.50 (GMT+7)
Workload	1. Lectures: 2 x 50 = 100 minutes per week. 2. Exercises and Assignments: 2 x 60 = 120 minutes (2 hours) per week. 3. Private learning: 2 x 60 = 120 minutes (2 hours) per week.
Credit points	2 credit points (sks)
Requirements according to the examination regulations	A student must have attended at least 75% of the lectures to sit in the exams.
Mandatory prerequisites	-
Learning outcomes and their corresponding PLOs	Course Learning Outcome (CLO) after completing this module, CLO-1 Able to understand the concept and basic techniques of image processing. CLO-2 Able to understand fundamental algorithm and how to implement it with programming language. CLO-3 Able to apply the said concept for more complex image processing applications individually or in groups.
Content	INTRODUCTION TO CRYPTOGRAPHY: an introduction to the basics of cryptography, data security, information theory, complexity and numbers. SOME ENCRYPTION ALGORITHMS: classical and modern encryption algorithms (DES and public key algorithms).

	CRYPTOGRAPHIC ENGINEERING: several cryptographic techniques, key management.
Study and examination requirements and forms of examination	• In-class exercises • Assignment 1, 2, 3 • Mid-term examination • Final examination
Media employed	LCD, whiteboard, websites (myITS Classroom), zoom.
Reading lists	Main: 1. William Stallings, Cryptography and Network Security, Principle and Practise. 2nd ed., Prentice Hall, 1999 2. Douglas R. Stinson, "Cryptography Theory and Practice", 3rd Edition, Chapman & Hall/CRC, 2006 Supporting: 1. Serge Vaudenay, "A Classical Introduction to Modern Cryptography', Springer, 2006 2. Rinaldi Munir "Kriptografi", Informatika Bandung