MODULE HANDBOOK
Master Program in Computer Science
Department of Computer Science and Electronics
Faculty of Mathematics and Natural Sciences
Universitas Gadjah Mada

Cryptology

Module name	**Cryptology**
Module level	Master
Code	MII-6816
Courses (if applicable)	Cryptology
Semester	1
Contact person	Drs. Retantyo Wardoyo, M.Sc., Ph.D.
Lecturer	Drs. Retantyo Wardoyo, M.Sc., Ph.D. Anny Kartika Sari, S.Si., M.Sc., Ph.D.
Language	Bahasa Indonesia
Relation to curriculum	master program, elective, 2nd semester.
Type of teaching, contact hours	Lectures, < 60 students Wednesday, 13.00-15.30.
Workload	1. Lectures: 3 x 50 = 150 minutes (2.5 hours) per week. 2. Exercises and Assignments: 3 x 60 = 180 minutes (3 hours) per week. 3. Private study: 3 x 60 = 180 minutes (3 hours) per week.
Credit points	3 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.
Recommended prerequisites	-
Learning outcomes and their corresponding PLOs	After completing this module, a student is expected to:

CO	Description	upported PLO
	e to explain general theories related to number theory.	
	le to explain classical cryptosystem algorithms.	PLO-3, PLO-4
	Be able to apply asymmetric cryptosystem algorithms (examples: Diffie-Helman, RSA, El Gamal).	PLO-3, PLO-4, PLO-5, PLO-6
	e to explain the application of modern cipher algorithms (examples: DES, AES, message authentication, digital signatures)	PLO-5, PLO-6, PLO-8, PLO-9
	to explain the concepts of steganography, the algorithms and its applications	PLO-4 PLO-5

		e to analyse cryptosystem using statistic probability and brute force.	PLO-4

Content	This course provides the students with the knowledge of cryptography and cryptanalisis.
Study and examination requirements and forms of examination	● In-class exercises ● Assignments ● Mid-term examinations ● Final examinations
Media employed	LCD, blackboard, and websites.
Assessments and Evaluation	

CO	Assessment method	Percentage	Total
CO-1	Assignment 1	5%	**5%**
CO-2	Assignment 2	5%	**45%**
	Assignment 3	10%	
	Question 1 of midterm exam	10%	
	Question 2 of midterm exam	10%	
	Question 3 of midterm exam	10%	
CO-3	Assignment 4	5%	**15%**
	Question 1 of final exam	10%	
CO-4	Assignment 5	5%	**15%**
	Question 2 of final exam	10%	
CO-5	Assignment 6	5%	**15%**
	Question 3 of final exam	10%	
CO-6	Assignment 7	10%	**5%**

Reading List	● Menezes, A, P. Van Ooschot, dan S. Vanstase, 1996, "Handbook of Applied Crypography", CRC Press. ● Stalling, W., 2011, "Cryptography and Network Security", Prentice Hall ● Brown, L, 2001, Crpytography and Computer Security, Australian Defense National Academy. ● Patterson, W., Mathematical Cryptology". ● Miller, M., "Short Course on Cryptography".