UNIVERSITAS GADJAH MADA

Faculty of Mathematics and Natural Sciences

Department of Computer Science and Electronics

Sekip Utara Bulaksumur Yogyakarta 55281 Telp: +62 274 546194 Fax: +62 274 546194 Email: dep-ike.mipa@ugm.ac.id

Doctoral Programme of Computer Science

Telephone	: (0274)546194
Email	: s3ik.mipa@ugm.ac.id
Website	: http://dcse.fmipa.ugm.ac.id/site/id/s3-ilmu-komputer/

Module name	: **C**RYPTOLOGY
Module level, if applicable	: **D**OCTORAL
Code, if applicable	: MII7265
Semester(s) in which the module is taught	: 1 (Odd)
Person responsible for the module	: Anny Kartika Sari, M.Sc., Ph.D.
Lecturer(s)	: Anny Kartika Sari, M.Sc., Ph.D. Retantyo Wardoyo, M.Sc., Ph.D
Language	: Indonesian
Relation to curriculum	: Elective course
Credit points	: 3
Type of teaching, contact hours	: Discussion, presentation
Workload	: a) Lectures (discussion and presentation): 14 x 3 hours = 42 hours, b) Projects, consisting of: - Experiments: 10 x 4 hours = 40 hours, and - Writing draft of publication: 10 x 5 hours = 50 hours.
Requirements according to the examination regulations	: A student must have at least 75% of attendance. The final score is evaluated based on the experiments (50%), and publication draft (60%).
Recommended prerequisite	: -
Module objectives/ intended learning outcomes	: CO1 : Student is up to date with the state-of-the-art of the methods related to security, cryptography and cryptology. CO2 : Student is able to analyse the problems related to security, cryptography and cryptology. CO3 : Student is able to formulate research problems related to security, cryptography and cryptology. CO4 : Student master the fundamental knowledge related to security, cryptography and cryptology.

	CO5 : Student is able to solve problems related to security, cryptography and cryptology through experiments.
Content	This course may cover the following topics. However, the focus of the discussion will be tailored according to student's research topic. 1. Concepts of cryptography, cryptanalysis, cryptology 2. Classical cryptography and cryptanalysis 3. Modern ciphers: block ciphers (AES), stream ciphers, chaos-based cryptography 4. Attacks on modern cryptography 5. Asymmetric cryptography: RSA, elliptic curve cryptography, lattice-based cryptography 6. Cryptanalysis of asymmetric cryptography 7. Homomorphic encryption 8. Message authentication and digital signatures 9. Steganography and watermarking 10. Cryptanalysis of hash function
Study and examination requirements and forms of examination	: Presentation and paper writing
Media employed	: Slides.
Reading List	1. Stalling, W., 2016, *Cryptography and Network Security: Principles and Practice*, Edisi ke-6, Prentice Hall 2. Boneh, D., Shoup, V., *A Graduate Course in Applied Cryptography*, 2020. 3. Swenson, C., *Modern Cryptanalysis*, Wiley Publishing, Inc., 2008.

The Mapping of COs to PLOs

COs	**PLO**s							
	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8
CO1				■				
CO2					■			
CO3						■		
CO4							■	
CO5								■

The PLO of DP-CS

PLO	**Knowledge Area**	**PLO Description**
PLO1	[Values and principles]	A graduate should be devoted to God Almighty, uphold the humanity values, internalize academic values and ethics, responsible in working around expertise independently.

Managerial Capability		
PLO2	[Professional attitudes]	A graduate should have good interpersonal skills; able to work together within the organization, both as a leader and a member; able to be the initiator; able to manage and delegate tasks; and have a sense of responsibility for their own work as well as take responsibility for the achievement of the organization's work.
PLO3	[Communication skills]	A graduate should be able to communicate effectively and efficiently with stakeholders from various backgrounds; use English well; and able to write and present scientific papers correctly and well.
PLO4	[Life-long learning]	A graduate should be up to date with the state-of-the-art especially in computer science field, able to take parts in the development of computer science field that is engaged in and relate it to other fields throughout life.
Working Capability		
PLO5	[Problem-solving and Scientific skills]	A graduate should be able to analyse science and technology problems in the computer science field, develop alternative solutions through intra disciplinary, interdisciplinary, and trans disciplinary approaches to produce innovative, original, and tested works.
PLO6	[Ability to formulate and do research]	A graduate should be able to formulate research problems through critical, exploratory, and innovative studies both independently and in groups of computer science field that is engaged in and present research results in a scientific paper at regional or international level.
Mastering Knowledge		
PLO7	[Fundamental knowledge]	A graduate should be able to develop knowledge in the field of computer science that is engaged, which includes abstraction, complexity, evolution and philosophy of changes or developments in the field of science.
PLO8	[Applied knowledge]	A graduate should be able to develop theoretical, philosophical, and applied concepts in the field of computer science that is engaged in, and to represent them in a structured and systematic manner.