UNIVERSITAS NEGERI YOGYAKARTA
FACULTY OF MATHEMATICS AND NATURAL SCIENCES
DEPARTMENT OF MATHEMATICS EDUCATION
Jalan Colombo Nomor 1 Yogyakarta 55281
Telepon(0274)565411 Pesawat 217, (0274)565411(TU),fax (0274)548203
Laman :fmipa.uny.ac.id, E-mail :humas_fmipa@uny.ac.id

Bachelor of Science in Mathematics

MODULE HANDBOOK

Module name:	Cryptography
Module level,if applicable:	Undergraduate
Code:	MAT6341
Sub-heading,if applicable:	-
Classes,if applicable:	-
Semester:	6th
Module coordinator:	Dwi Lestari, M.Sc.
Lecturer(s):	Dwi Lestari, M.Sc.
Language:	Bahasa Indonesia
Classification within the curriculum:	Elective course
Teaching format / class hoursperweekduring the semester:	150 minutes lectures and 180 minutes structured activities per week.
Workload:	Total workload is 136 hours per semester which consists of 150 minutes lectures, 180 minutes structured activities, and 180 minutes self-study per week for 16 weeks.
Creditpoints:	3
Prerequisites course(s):	Number Theory(MAT6205)
Courseoutcomes:	After taking this course the students have ability to: CO1. Appreciate the work and opinions of other groups in submitting ideas in writing or verbally CO2. Demonstrate collaborative attitude and independence in carrying out independent tasks and group assignments CO3. Communicate ideas in solving mathematical problems in

	writing or verbally
	CO4. Explain the information security theory and examples of its application in information technology.
	CO5. Use algorithms to solve related problems
	CO6. Use computer software to run algorithms
Content:	This course discusses the basics of cryptography, classical cryptography, Data Encryption Standard (DES), Advanced Encryption Standard (AES), public key, RSA, Elgamal, discrete logarithms, email and internet security.
Study/exam achievements:	CO1: Attitude assessment is carried out at each meeting by observation and / or self-assessment techniques using the assumption that basically every student has a good attitude. The student is given a value of very good or not good attitudeif they show it significantlycompared to other students in general. The result of attitude assessment is not a component of the final grades, but as one of therequirements to pass the course. Students will pass from this course if at least have a good attitude.

The final mark will be weight as follow:

No	CO	Assesment Object	Assessment Techniques	Weight
1	CO 1, CO 3	Group Presentation	Observation/ presentation test	30%
2	CO 2	Collaborative skills	Observation	10%
3	CO 4, CO 5, CO 6	a. Individual assignments and group assignments b. Final Exam	Written Test	25 % 35%
			Total	100%

Forms of media:	Board, LCD Projector, Laptop/Computer
Literature:	1. Mollin, A.R. 2007. *An Introduction to Cryptography*. Chapman&Hall/CRC : New York 2. Stinson, D.R. 2006. *Cryptography; Theory and Practice*. Chapman&Hall/CRC : New York

PLO and CO mapping

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6	PLO7	PLO8	PLO9	PLO10
CO1		✓								
CO2			✓							
CO3				✓						
CO4					✓					
CO5								✓		
CO6										✓