UNIVERSITAS GADJAH MADA
Faculty of Mathematics and Natural Sciences
Mathematics Department
Sekip Utara BulaksumurYogyakarta 55281Telp: +62 274 552243 Fax: +62 274 555131 Email: math@ugm.ac.id Website: http://math.fmipa.ugm.ac.id

Undergraduate Programme in Mathematics
Telp : +62 274 552243
Email : maths1@ugm.ac.id; kaprodi-s1-matematika.mipa@ugm.ac.id
sekprodi-s1-matematika.mipa@ugm.ac.id
Website : http://s1math.fmipa.ugm.ac.id/

MODULE HANDBOOK

Module name	Introduction to Cryptography
Module level, if applicable	Bachelor
Code, if applicable	MMM-4206
Subtitle, if applicable	-
Courses, if applicable	Introduction to Cryptography
Semester(s) in which the module is taught	7th (seventh)
Person responsible for the module	Algebra Research Group
Lecture	Dr. Diah Junia Eksi Palupi, MS
Language	Bahasa Indonesia
Relation to curriculum	Elective Course
Type of teaching, contact hours	150 minutes lectures per week, 180 minutes supervised activities per week, 180 minutes individual learning per week.
Workload	Total workload is 136 hours per semester, which consists of 150 minutes lectures per week for 14 weeks, 180 minutes structured activities per week, 180 minutes individual study per week, in total is 16 weeks per semester, including mid exam and final exam.
Credit points	3
Requirements according to the examination regulations	Students have taken Introduction to Cryptography course (MMM-4206) and have an examination card where the course is stated on.
Recommended prerequisites	Students have taken Introduction to Linear Algebra course (MMM-2202) and have participated in the final examination of the course.
Module objectives/intended learning outcomes	Upon successful completion, CO 1. Students are able to comprehend the cryptosystem and to construct the ciphermodel of a problem. CO 2. Students are able to comprehend the cryptanalysis and to apply for some populer ciphers. CO 3. Students are able to comprehend the Multicryptosystem and to build the cryptosystem of some famous systems. CO 4. Students are able to comprehend some kind public-key systems and to implement to solve some daily problems. CO 5. Students are able to comprehend a secret scheme and to implement for some familiar systems.
Content	Cryptology, cryptosystem and cryptanalysis. Cipher; Shift, Substitution, Affine, Vigenere, Hill, Permutation, Stream. Cryptanalysis of that ciphers. Multicryptosystem, Entropi and its properties, Block cipher, DES and AES, Hash function. Public key cryptosystem RSA, Cina reminder theorem, prima test, EL Gamal, Elliptic curve. Signatures scheme of RSA and El Gamal.
Study and examination requirements and forms of examination	The final mark will be computed from a proportional weight of assignments, mid examination and final examination. The final mark will be weighted as follows: No — Assessment methods (components, activities) — Weight (percentage) 1 — Final Examination — 40% 2 — Mid-Term Examination — 35% 3 — Class Activities: Quiz, Homework, etc. — 25% The initial cut-off points for grades A, B, C, and D should not be less than 80%, 70%, 50%, and 40%, respectively.

Media employed	Boards, projectors.
Reading List	1. Katz J., Lindell Y., 2015, *Introduction to Modern Cryptography, 2nd Edition,* CRC Press Taylor and Francis Group, U.S. 2. Hoffstein, J., Pipher, J., Silverman, H.J., 2014, *An Introduction to Mathematical Cryptography (Undergraduate Text in Mathematics)*, Springer Science-Bussines Media, New York 3. Jonathan Katz, Yehuda Lindell, 2014, *Introduction to Modern Cryptography*, Taylor and Francis. 4. E Douglas R. Stinson, 2002, *Cryptography Theory and Practice,* 2ndEd, A CRC Press Company, Boca Raton, London, New York, Washington DC. 5. Johannes A. Buchmann, 2001, *Introduction to Cryptografi,* Springer-Verlag, New York, Berlin, Heidelberg. 6. Wayne Patterson, 1987, *Mathematical Cryptology for computer scientics and Mathematicians*, Rowman & Littlefield, United States of America.

PLO and CO Mapping

	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5	PLO 6	PLO 7	PLO 8	PLO 9
CO 1		v			v				
CO 2		v	v		v				
CO 3			v		v				
CO 4			v		v				
CO 5			v	v	v	v			v