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

Master in Mathematics
Telp : +62 274 552243
Email : maths2@ugm.ac.id; kaprodi-s2-matematika.mipa@ugm.ac.id
sekprodi-s2-matematika.mipa@ugm.ac.id
Website : http://s2math.fmipa.ugm.ac.id/

MODULE HANDBOOK

Module Name	Cryptography
Module level, if applicable	Master
Code, if applicable	MMM 6208
Subtitle, if applicable	Cryptography
Courses, if applicable	Cryptography
Semester(s) in which the module is taught	2nd or 4th
Person responsible for the module	Chair of Algebra Research Group
Lecturer(s)	Indah Emilia Wijayanti, Diah Yunia Eksi Palupi
Language	Bahasa Indonesia
Relation to curriculum	Elective course. Related to : Algebraic Structure
Teaching methods	Lecture, project based.
Workload (incl. contact hours, self-study hours)	Total workload: 3 hours lectures, 3 hours supervised activities, 3 hours individual learning per week, 14 weeks per semester, total 9 hours x 14 weeks = 126 hours per semester. Contact hours: 3 hours lectures per week. Private study including examination preparation, specified in hours: 3 hours individual per week.
Credit points	3

Required and recommended prerequisites for joining the module	Algebraic Structure
Module objectives/intended learning outcomes	After the course the student should be able to : CO1. demonstrate knowledge and understanding of basic notions in cryptography, CO2. identify some mathematical problems and the associated mathematical theory that underlies the asymmetric cryptographic applications treated in the course, and to solve problems using this theory, CO3. demonstrate knowledge and understanding the algorithms that are treated in the course, and account for and prove their complexity, CO4. implement the simpler of these algorithms using mathematical software, and to analyze their complexity in practice.
Content	The course treats basic notions in cryptography and the mathematical problems, with associated mathematical theory, that are the basis for asymmetric cryptographical applications such as RSA (both as cryptosystem and digital signature), DH, El Gamal, ECDH, ECDSA and Miller-Rabin. Different algorithms (to solve these mathematical problems) are studied with a focus on their complexity. Algorithms that are treated include fast powering, Shank's baby-step giant-step, Pohlig-Hellman, Pollard's p-1, QS, index calculus, Pollard's rho och Lenstra's ECM.
Examination forms	Oral presentation, essay.

Study and examination requirements	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 — 20 – 30 % 2 Mid-Term Examination — 20 – 30 % 3 Project — 50 - 55 % **Minimum final mark to pass : 60 (C).**
Media employed	Whiteboard, computer, LCD, online platform.
Reading list	1. E Douglas R. Stinson, 2002, CryptographyTheory and Practice, 2nd Ed, A CRC Press Company, Boca Raton, London, New York, Washington DC. 2. Johannes A. Buchmann, 2001, Introduction to Cryptografi, Springer-Verlag, New York, Berlin, Heidelberg. 3. Wayne Patterson, 1987, Mathematical Cryptology for computer scientics and Mathematicians, Rowman & Littlefield, United States of America. 4. Katz J., Lindell Y., 2015, Introduction to Modern Cryptography, 2nd Edition, CRC Press Taylor and Francis Group, U.S. 5. Hoffstein, J., Pipher, J., Silverman, H.J., 2014, An Introduction to Mathematical Cryptography (Undergraduate Text in Mathematics), Springer Science-Bussines Media, New York 6. William Stallings, Cryptography and Network Security Principle and Practice, Pearson Education Inc., 6th Edition, 2014. 7. Bruce Schneier, Applied Cryptography Protocols, Algorithms, and Source Code in C, Wiley Publication, 2nd Edition, 1996.

CO-PLO MAPPING

	PLO1	PLO2	PLO3	PLO4	PLO5	PLO6
CO 1	V		V	V	V	V
CO 2	V		V	V	V	V
CO 3	V		V	V	V	V
CO 4	V		V	V	V	V

Compilation Date : **29 Juli 2022**

Modified Date : **29 Juli 2022**

Learning Outcomes

Knowledge and Understanding

Having successfully completed this module, you will be able to demonstrate knowledge and understanding of:

- The historic struggle between code-makers and code-breakers
- The broad categories of codes and ciphers, and appropriate uses for each

Subject Specific Practical Skills

Having successfully completed this module you will be able to:

- Select appropriate ciphers, cipher modes, and protocols for simple applications
- Attack classical ciphers such as Vigenère, and LFSR-based stream ciphers

Subject Specific Intellectual and Research Skills

Having successfully completed this module you will be able to:

- Perform simple mathematics appropriate to public-key encryption, and to cryptosystems based on polynomials over the binary numbers

Transferable and Generic Skills

Having successfully completed this module you will be able to:

- Use graduate-level literature to investigate areas of mathematics previously unfamiliar to you