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

Magister Programme 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	Topics in Algebra C
Module level, if applicable	Magister
Code, if applicable	MMM-6213
Subtitle, if applicable	Max Plus Algebra
Courses, if applicable	Kapita Selekta Aljabar C (Aljabar Max Plus)
Semester(s) in which the module is taught	!st (first) or 3rd (third)
Person responsible for the module	Head of Algebra Research Group
Lecturer	Dr. Ari Suparwanto, Dr. Diah Yunia Eksi Palupi
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 apply max plus algebra comprehend some kind public-key systems and to implement to solve some daily problems.
Content	Finite field, polynomial ring; computational complexity; cryptosystem, Hash function, public key cryptosystem RSA,SHA, AES, El Gamal, Elliptic curve, Signatures scheme of RSA and El Gamal, randomness RNG, PRNG; Introduction to distributed ledger/block chain, post quantum cryptography, privacy preserving (zero knowledge); max plus algebra, max plus algebra cryptography.
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 — 20 - 30% 2 — Mid-Term Examination — 20 - 30% 3 — Class Activities: Quiz, Homework, etc. — 50 - 55% Minimum final mark to pass : 60 (C).
Media employed	Boards, projectors, computer.

Reading List	1. E Douglas R. Stinson, 2002, *Cryptography Theory 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. Whitfield Diffie and Martin E. Hellman, 1976, New directions in cryptography, *IEEE Transactions on Information Theory*, vol. It-22 no. 6, 644 – 654. 5. R. L. Rivest, A. Shamir, and L. Adleman, 1978, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communication of the ACM*, Vol 21 No 2, 120-126. 6. Lidong Chen and Dustin Moody, 2020, New Mission and Opportunity For Mathematics Researchers: Cryptography In The Quantum Era, *Advances in Mathematics of Communications*, Vol 14 No. 1, 161–169. 7. Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen, *Post-Quantum Cryptography*, Springer-Verlag, Berlin, 2009. 8. Adi Shamir, 1979, *How to Share a Secret,* Communication of the ACM, Vol 22 No 11, 612-613. 9. Ling San and Chaoping Xing, *Coding Theory A First Course*, Cambridge University Press, 2004

PLO and CO Mapping

	PLO 1	PLO 2	PLO 3	PLO 4	PLO 5	PLO 6
CO 1	√		√			
CO 2			√		√	√
CO 3	√		√		√	√
CO 4	√		√		√	√