SHIVAJI UNIVERISTY, KOLHAPUR-416 004. MAHARASHTRA
PHONE : EPABX-2609000 **website- www.unishivaji.ac.in**
FAX 0091-0231-2691533 & 0091-0231-2692333 – BOS - 2609094
शिवाजी विद्यापीठ, कोल्हापूर – 416004.
दुरध्वनी (ईपीएबीएक्स) २६०९००० (अभ्यास मंडळे विभाग– २६०९०९४)
फॅक्स : ००९१-०२३१-२६९१५३३ व २६९२३३३.e-mail:bos@unishivaji.ac.in

Estd. 1962
NAAC 'A' Grade

SU/BOS/Science/ No 0 0 3 9 7 **Date:** 1 8 OCT 2021

To,

1) The Principal, All Concerned Affiliated Colleges/Institutions Shivaji University, Kolhapur	2) The Head, All Concerned Department Shivaji University, Kolhapur.

Subject: Regarding Syllabi of **M.Sc Part II Mathematics Sem IV** under the Faculty of Science and Technology.

Sir/Madam,

With reference to the subject mentioned above, I am directed to inform you that the University authorities have accepted and granted approval to the revised syllabi of **M.Sc Part II Mathematics Sem IV** under the Faculty of Science and Technology.

Sr.No	Titile of Paper	Course Code
1	**Introduction to Cryptology**	CCS-403, CCS-404, CCS-405
2	**Advanced Algebra**	

This syllabi shall be implemented from the academic year 2021-2022 (i.e. from June 2021) onwards. A soft copy containing the syllabus is attached herewith and it is also available on university website **www.unishivaji.ac.in**)

You are, therefore, requested to bring this to the notice of all students and teachers concerned.

Thanking you,

Yours faithfully,

Dy Registrar

Copy to:

1	The Dean, Faculty of Science & Technology	7	Appointment Section
2	The Chairman BOS	8	Computer Centre
3	B.Sc/M.Sc Section	9	Affiliation Section (U.G.)
4	O.E. II, Section	10	Affiliation Section (P.G.)
5	Eligibility Section	11	P.G.Admission Section
6	P.G.Seminar Section		

M.A. / M.Sc. (Mathematics) Part -II (Semester III)

Course code	Title of course
CCS-403, CCS-404, CCS-405	18. Advanced Algebra 19. Introduction to Cryptology

M. A. / M. Sc. Mathematics (Part II) (Semester IV)
(Choice Based Credit System)
(Introduced from June 2021 onwards)

Course Code: CCS-403, CCS-404, CCS-405
Title of Course: Advanced Algebra
Course Outcomes: Upon successful completion of this course, the student will be able to:

1. classify the ideals to solve the related problems.
2. understand Artinian and Noetherian modules.
3. apply integral extensions for going up and going down theorem
4. use Nakayama Lemma for further development in Noetherian

Unit I: Zero-divisors. Nilpotent elements. Units, Prime ideals and maximal ideals, Nilradical and Jacobson radical, Operations on ideals, Extension, and contraction. **15 Lectures**

Unit II : Operations on submodules, Direct sum and product of submodules, Finitely generated modules, Exact sequences, Tensor product of modules.

15 Lectures

Unit III : Integral dependence, The going-up theorem. Integrally closed integral domains. The going-down theorem, Chain conditions. **15 Lectures**

Unit IV: Primary decomposition in Notherian rings, Artinian rings, Discrete valuation rings, Dedekind domains ,Fractional ideals **15 Lectures**

Unit V: Examples, seminars, group discussions on the above four units. **15 Lectures**

Recommended Book:

M. F. Atiyah and I. G. MacDonald – Introduction to Commutative Algebra, Addison Wesley publishing company

Reference Books :

1. M. D. Larsen and P. J. McCarthy: Multiplicative theory of ideals, Academic press, 1971

2 .D. G. Northcot, Ideal theory, Cambridge University, press, 1953

3. Oscar Zariski and P. Samual – Commutative Algebra, Vol I, Affiliated East West press pvt. Ltd. New Delhi.

M. A. / M. Sc. Mathematics (Part II) (Semester IV)
(Choice Based Credit System)
(Introduced from June 2021 onwards)

Course Code: CCS-403, CCS-404, CCS-405

Title of Course: Introduction to Cryptology

Course Outcomes: Upon successful completion of this course, the student will be able to:

1. Apply specialized knowledge in cryptography to solve network security problems.
2. Gain an advanced and integrated understanding of the fundamentals of and interrelationship between mathematics and cryptography.
3. Gain a comprehensive introduction to the history of cryptography, known attacks on cryptosystems.

Unit I: Classical cryptography and Shannon's Theory: Introduction to Caeser Cipher, modular arithmetic, the Shift cipher, Affine Cipher, Vigenere Cipher, Perfect secrecy, Application of Shift Cipher **15 Lectures**

Unit II : Block Cipher : Product Cipher, Block Cipher, Modes of Operation for Block Cipher, Suubstitution Permtation Network, Fiestel Cipher, S-Box Theory, Cryptanalysis and its Variants, Linear Attack **15 Lectures**

Unit III : **Public Key Cryptology :** RSA Cryptosystem, Complexity analysis of Euclidean Algorithm ad RSA Cryptosystem, square and multiply algorithm, Primality testing-Miller-Rabin Algorithm, Legendre Symbol and Jacobi Symbol, Solovay-Stassen Algorithm **15 Lectures**

Unit IV: **Cryptographic Hash Function :** Introduction, Random Oracle Model, Security of hash functions, Randomized Algorithm and its application on Preimage resistance and collision resistance, Iterated Hash Functions. **15 Lectures**

Unit V: Examples, seminars, group discussions on the above four units. **15 Lectures**

Recommended Book:

Stinson D.,"Cryptography Theory and Practice", 3rd;edition, Chapman & Hall / CRC

Reference Books

1. Das A. and Venimadhavan C.E.,"Public-Key Cryptography-Theory, and Practice", Pearson Education Inc 3.Koblitz N.,"A Course in Number Theory and Cryptography", 2nd edition,Springer (Indian Reprint)
2. K. L. Chung: Elementary Probability Theory and Stochastic Processes, Springer-Verlag, New York, 1974. 4. S. M. Ross: Stochastic Processes, John Wiley, New York, 1983.
3. D. Boneh and V. Shoup : A Graduate Course in Applied Cryptography *(free)*