(Annexure-I)

UNIVERSITY OF DELHI

M.A./M.Sc. MATHEMATICS
SEMESTER SYSTEM

TWO-YEAR FULL TIME PROGRAMME

RULES, REGULATIONS AND COURSE CONTENTS

Department of Mathematics
Faculty of Mathematical Sciences
University of Delhi
Delhi-110007
2012

Syllabus applicable for the students seeking admission to the M.A./M.Sc. Mathematics course in the Academic Year 2012-2013

University of Delhi

Examination Branch

Date: 01.05.2012

Check List of Course Evaluation for AC Consideration

S.No.	Parameters	Status
1.	Affiliation	√
2.	Programme Structure	√
3.	Codification of Papers	√
4.	Scheme of Examinations	√
5.	Pass Percentage & Promotion Criteria	√
6.	Reappearance in Passed Papers	√
7.	Division Criteria	√
8.	Qualifying Papers	X
9.	Span Period	√
10.	Attendance Requirements	X
11.	Course Content of Each Paper	√
12.	List of Readings	√

MASTER OF ARTS / SCIENCE
(MATHEMATICS)

TWO-YEAR FULL-TIME PROGRAMME

AFFILIATION

The proposed programme shall be governed by the Department of Mathematics, Faculty of Mathematical Sciences, University of Delhi, Delhi-110007.

PROGRAMME STRUCTURE

The master's programme in Mathematics is divided into two parts as hereunder. Each part will consist of two semesters.

Part I	First Year	Semester – 1	Semester – 2
Part II	Second Year	Semester – 3	Semester – 4

The courses prescribed for various semesters shall be the following:

PART I: Semester-1

Math 101 – Complex Analysis
Math 102 – Functional Analysis
Math 103 – Field Theory
Math 104 – Differential Equations

PART I: Semester-2

Math 201 – Topology
Math 202 – Measure and Integration
Math 203 – Module Theory
Math 204 – Fluid Dynamics

PART II: Semester-3

Math 301: Any course out of the following

(i) Advanced Complex Analysis
(ii) General Measure Theory
(iii) General Topology

JBL

Math 302: Any course out of the following

(i) Fourier Analysis
(ii) Matrix Analysis
(iii) Theory of Operators
(iv) Computational Methods for Ordinary Differential Equations

Math 303: Any course out of the following

(i) Introduction to Algebraic Topology
(ii) Advanced Group Theory
(iii) Representation of Finite Groups
(iv) Computational Fluid Dynamics

Math 304: Any course out of the following

(i) Coding Theory
(ii) Mathematical Programming
(iii) Graph Theory
(iv) Methods of Applied Mathematics

PART II: Semester-4

Math 401: Any course out of the following

(i) Differential Geometry
(ii) Commutative Algebra
(iii) Calculus on R^n

Math 402: Any course out of the following

(i) Abstract Harmonic Analysis
(ii) Advanced Functional Analysis
(iii) Theory of Frames
(iv) Operators on Hardy-Hilbert Spaces
(v) Computational Methods for Partial Differential Equations

Math 403: Any course out of the following

(i) Homology Theory
(ii) Theory of Non-commutative Rings
(iii) Algebraic Number Theory
(iv) Advanced Fluid Mechanics

Math 404: Any course out of the following

(i) Advanced Coding Theory
(ii) Optimization Techniques and Control Theory
(iii) Cryptography

NOTES : (1) Each course will have 5 credits: 4 lectures, 1 discussion and 1 tutorial per week.

(2) In the beginning of the respective semesters, the department will announce the list of elective courses which will be offered during the semester depending upon the availability of lecturers and the demand of electives.

SCHEME OF EXAMINATION

1. English shall be the medium of instruction and examination.

2. Examinations shall be conducted at the end of each semester as per the Academic Calendar notified by the University of Delhi.

3. Each course will carry 100 marks and have two components: Internal Assessment 30% marks and End-Semester Examination 70% marks.

4. The system of evaluation shall be as follows:

 4.1 Internal assessment will be based on classroom participation, seminar, term courses, tests, quizzes. The weightage given to each of these components shall be decided and announced at the beginning of the semester by the individual teacher responsible for the course. No special classes will be conducted for a student during other semesters, who fails to participate in classes, seminars, term courses, tests, quizzes and laboratory work.

 4.2 The remaining 70 marks in each paper shall be awarded on the basis of a written examination at the end of each semester. The duration of written examination for each paper shall be three hours.

5. Examinations for courses shall be conducted only in the respective odd and even Semesters as per the Scheme of Examinations. Regular as well as Ex-students shall be permitted to appear / re-appear / improve in courses of Odd Semesters only at the end of Odd Semester and courses of Even Semesters only at the end of Even Semesters.

PASS PERCENTAGE & PROMOTION CRITERIA

(a) The minimum marks required to pass any paper in a semester shall be 40% in theory and 40% in Practical, wherever applicable. The student must secure 40% in the End Semester Examination and 40% in the total of End Semester Examination & Internal Assessment of the paper for both theory & practical separately.

(b) No student will be detained in I or III Semester on the basis of his / her performance in I or III Semester examination; i.e. the student will be promoted automatically from I to II or III to IV Semester respectively.

(c) A student shall be eligible for promotion from 1st year to 2nd year of the course provided he / she has passed 50% papers of I and II Semester taken together. However, he / she will have to clear the remaining paper/s while studying in the 2nd year of the programme.

(d) Students who do not fulfill the promotion criteria (c) above shall be declared fail in the part concerned. However, they shall have the option to retain the marks in the papers in which they have secured Pass marks as per Clause (a) above.

(e) A student who has to reappear in a paper prescribed for Semester I/III may do so only in the odd Semester examinations to be held in November/December. A student who has to reappear in a paper prescribed for Semester II/IV may do so only in the even Semester examinations to be held in April/May.

REAPPEARANCE IN PASSED PAPERS

(a) A student may reappear in any theory paper prescribed for a semester, on foregoing in writing her / his previous performance in the paper(s) concerned. This can be done once only in the immediate subsequent semester examination only (for example, a student reappearing in a paper prescribed for Semester I examination, may do so along with the immediate next Semester III examinations only).

(b) A candidate who has cleared the papers of Part II (III & IV Semester) may reappear in any paper of Semester III or IV only once, at the immediate subsequent examination on foregoing in writing his / her previous performance in the paper(s) concerned, within the prescribed span period.

(Note: The candidate of this category will not be eligible to join any higher course of study)

(c) In the case of reappearance in a paper, the result will be prepared on the basis of candidate's current performance in the examination.

(d) In the case of a candidate, who opts to re-appear in any paper(s) under the aforesaid provisions, on surrendering her / his earlier performance but fails to re-appear in the paper(s) concerned, the marks previously secured by the candidate in the paper(s) in which he / she has failed to re-appear shall be taken into account while determining her/ his result of the examination held currently.

(e) Reappearance in practical examinations, dissertation, project and field work shall not be allowed.

(f) A student who reappears in a paper shall carry forward the internal assessment marks, originally awarded.

DIVISION CRITERIA

A student who passes all the papers prescribed for Parts I & II examinations would be eligible for the degree. Such a student shall be categorized on the basis of the combined result of Parts I & II examinations as follows:-

60% or more	First Division
50% or more but less than 60%	Second Division
40% or more but less than 50%	Third Division

SPAN PERIOD

No student shall be admitted as a candidate for the examination for any of the semesters after the lapse of four years from the date of admission to Semester-1 of the Master's programme in Mathematics.

Math 101 - Complex Analysis

Analytic functions as mappings, conformal mappings, Mobius transformations, branch of logarithm.

Riemann-stieltjes integrals, power series representation of analytic functions, zeros of analytic functions, maximum modulus theorem, Cauchy's theorem and integral formula on o pen subsets of C, the homotopic version of Cauchy's theorem and simply connectedness, counting zeros, open mapping theorem, Goursat'stheorem, maximum principle, schwarz's lemma.

Classification of singularities, Laurent series , residues, contour integration, argument principle, Rouche's theorem.

References:

[1] L.V. Ahlfors, Complex Analysis, McGraw Hill Co., New York, 1988.

[2] J. B. Conway, Functions of one complex variable, Narosa, Delhi, 2000.

[3] T. W. Gamelin, Complex Analysis, Springer-Verlag, 2008.

[4] S. Lang, Complex Analysis, Springer-Verlag, 2003.

Math 102 - Functional Analysis

Normed spaces, Banach spaces, properties of normed spaces, finite dimensional normed spaces and subspaces, compactness and finite dimension, linear operators, bounded and continuous linear operators, linear functionals, linear operators and functionals on finite dimensional spaces, normed spaces of operators, dual spaces.

Inner product spaces, Hilbert spaces, properties of inner product spaces, orthogonal complements and direct sums, orthonormal sets and sequences, series related to orthonormal sequences and sets, total orthonormal sets and sequences, representation of functionals on Hilbert spaces, Hilbert-adjoint operator, self-adjoint, unitary and normal operators.

Hahn-Banach theorems for real/complex vector spaces and normed spaces, application to bounded linear functionals on C[a,b], adjoint operators, reflexive spaces, category theorem, uniform boundedness theorem, strong and weak convergences, open mapping theorem, closed graph theorem.

Spectrum of an operator and its non-emptiness.

References:

[1] Erwin Kreyszig, Introductory Functional Analysis with Applications, John Wiley and Sons (Asia), Pvt. Ltd., 2006.

[2] George Bachman and Lawrence Narici, Functional Analysis, Dover, 2000.

[3] John B. Conway, A course in Functional Analysis, second edition, Springer-Verlag, 2006.

[4] Martin Schechter, Principles of Functional Analysis, second edition, AMS Book store, 2002.

[5] V.S. Sunder, Functional Analysis, Spectral Theory, Birkhauser Texts, Basel, 1997.

Fields and their extensions, splitting fields, the algebraic closure of a field, separability, automorphisms of field extensions, the fundamental theorem of Galois theory, roots of unity, finite fields, primitive elements; Galois theory of equations, the solution of equations by adicals.

References:

[1] P M. Cohn, Classic Algebra, John Wiley & Sons Ltd., 2000.
[2] P M. Cohn. Basic Algebra, Springer International Edition, 2003
[3] N Jacobson, Basic Algebra I and II, Hindustan Publishing Co., 1989.
[4] T.W Hungerford, Algebra, Springer-Verlag, 1981.

Math 104 - Differential Equations

Existence and uniqueness of solution of ordinary differential equation of first order. Picard's method. Existence theorem in complex plane. Existence and uniqueness theorem for simultaneous differential equations of first order. Existence and uniqueness theorem for ordinary differential equation of higher order. Sturm comparison and separation theorems, Homogeneous linear systems, Nonhomogeneous Linear systems, linear systems with constant coefficients.Two point boundary value problems, Greens function, construction of Green functions, Sturm-Lioville systems, Eigen values and Eigen functions.

Stability of autonomous system of differential equations, critical point of an autonomous system and their classification as stable, asymptotically stable, strictly stable and unstable.Stability of linear systems with constant coefficients. Linear plane autonomous systems, perturbed systems. Method of Lyapunov for nonlinear systems.

Solution of PDEs by method of integral transforms (Laplace and Fourier).Boundary value problems, Maximum and minimum principles, Uniqueness and continuity Theorems. Laplace equation in two-dimensions, Dirichlet and Neumann problem for half plane, Dirichlet and Neumann problem for a circle, Green's function for Laplace equation in two dimensions, Dirichlet problem for sphere and semi-infinite space, Greens function for three-dimensional Laplace equation.

Wave equation, Helmholtz's first and second theorems. Green's function for wave equation. Duhamel's principles for wave equation.

Diffusion equation, Solution of initial boundary value problems for the diffusion equation, Green's function for diffusion equation.
Duhamel's principles for heat equation.

References:

1. G.F.Simmons: Ordinary Differential Equations with applications and Historical notes *McGraw-Hill, 1991.*
2. Ian Sneddon, Elements of Partial Differential Equations, *McGraw-Hill* 1986
3. Tyn-MynT.U, Ordinary Differential Equations, Elsevier North-Holland, 1978
4. Tyn MynT.U, Linear Partial Differential Equations for Scientists and Engineers, Birkhauser, 2007.
5. S.L.Ross, Differential Equation, Wiley India, 2004

Math 201 - Topology

Topological spaces, interior, closure and boundary of a set, basis and subbasis for a topology, order topology, subspaces, continuous functions, homeomorphism, product topology, metrizability of products of metric spaces, quotient topology. Convergence: sequences and nets. T_1 and T_2 separation axioms, Connectedness, components, local connectedness, path connectedness, path components, local path connectedness. First countability, second countability, separability and Lindelöf conditions. Compactness, Bolzano-Weierstrass property, sequential compactness, local compactness and one-point compactification.

References:

[1] G. Bredon, Topology and Geometry, Springer-Verlag, 2005.
[2] J. Dugundji, Topology, Allyn and Bacon, 1970.
[3] J.L. Kelley, General Topology, Springer–Verlag, 2005.
[4] J. R. Munkres, Topology, second edition, Pearson Education, 2003.
[5] S. Willard, General Topology, Dover Publications, inc. N.Y., 2004..

Math 202 - Measure and Integration

Lebesgue outer measure, measurable sets, regularity, measurable functions, Borel and Lebesgue measurability, non-measurable sets

Integration of nonnegative functions, the general integral, integration of series, Riemann and Lebesgue integrals.

Functions of bounded variation, Lebesgue differentiation theorem, differentiation and integration, absolute continuity of functions.

Measures and outer measures, measure spaces, integration with respect to a measure.

The L^p spaces Hölder and Minkowski inequalities, completeness of L^p spaces, Convergence in measure, almost uniform convergence, Egorov's theorem.

References :

[1] G. De Barra, Measure Theory and Integration, Wiley Eastern Ltd. 1981.

[2] E. Hewitt and K. Stromberg, Real and Abstract Analysis, Springer, Berlin, 1988.

[3] H. L. Royden, Real Analysis, Pearson, 2008.

Math 203- Module Theory

Modules, Basic Concepts, Direct product and Direct sums, Exact sequences, Split exact sequences, Five lemma, Free modules, Modules over P.I.D., Nakayama lemma, Tensor product of modules, Categories and Functors, Hom functors, Semi simple modules, Projective and Injective modules, Baer's criterion, Divisible modules.

References:

1. P.M. Cohn, Classic Algebra, John Wiley & Sons Ltd., 2000.
2. P.M. Cohn, Basic Algebra, Springer International Edition, 2003.
3. D. S. Dummit & R.M. Foote, Abstract Algebra, Wiley India Pvt. Ltd.
4. T.W. Hungerford, Algebra, Springer-Verlag, 1981.
5. N. Jacobson, Basic Algebra, Volume II, Hindustan Publishing Co., 1989.

Math 204 - Fluid Dynamics

Classification of fluids, the continuum model, Eulerian and Lagrangian approach of description. Differentiation following fluid motion. Irrotational flow,vorticity vector, equi-potential surfaces. Streamlines, pathlines, streak lines of the particles, stream tube and stream surface. Mass flux density, conservation of mass leading to equation of continuity. (Euler's form.), Origin of forces in fluid. Conservation of momentum and its mathematical formulation: Euler's form. Integration of Euler's equation under different conditions. Bernoulli's equation, steady motion under conservative body forces. Boundary surface.

Theory of irrotational motion, Kelvin's minimum energy and circulation theorem, potential theorems. Some two and three dimensional flows, sources, sinks, doublets and vortices ,their images with respect to a plane and sphere. Milne –Thompson circle theorem, Butlers sphere theorem, Kelvin's inversion theorem and Weiss's sphere theorem. Axi-symmetric flows and stream function. Motion of cylinders and spheres. Two dimensional flows of irrotational, incompressible fluids, complex potential and its applications to two dimensional singularities. Blasius theorem, D'Alembert's paradox

Viscous flow, stress and strain analysis. Stokes hypothesis, The Navier-Stokes equations of motion. Some exactly solvable problems in viscous flows, steady flow between parallel plates, Poiseuille flow, steady flow between concentric rotating cylinders.

REFERENCES

1. P.K. Kundu and I.M. Cohen, Fluid Mechanics, Academic Press,2005.
2. L.M.MilneThomson, Theoretical Hydrodynamics, The Macmillan company, USA,1969.
3. N.E.Neill and F. Chorlton, Ideal and incompressible fluid dynamics, Ellis Horwood Ltd, 1986.
4. N.E.Neill and F. Chorlton, Viscous and compressible fluid dynamics, Ellis Horwood Ltd, 1986.
5. D.E.Rutherford: Fluid Dynamics, Oliver and Boyd Ltd, London.1978.
6. F.Chorlton: text book of fluid dynamics, CBS,2004

Math 301 (i) - Advanced Complex Analysis

Hadamard's three circles theorem, Phragmen-Lindelöf theorem.

The space of continuous functions C(G, Ω), spaces of analytic functions, Hurwitz's thorem, Montel's theorem, spaces of meromorphic functions, Riemann mapping theorem, Weierstrass' factorization theorem, factorization of the sine function, the gamma function, the Riemann zeta function, the Riemann functional equation.

Runge's theorem, simply connected regions, Mittag-Leffler's theorem.

Harmonic functions, maximum and minimum principles, harmonic functions on a disk, Harnack's theorem, sub-harmonic and super-harmonic functions, maximum and minimum principles, Dirichlet problem, Green's function.

References :

[1] J. B. Conway, Functions of one complex variable, Narosa Publishing House, New Delhi, 2000.

[2] T. W. Gamelin, Complex Analysis, Springer-Verlag, 2008.

[3] L. Hahn and B. Epstein, Classical Complex Analysis, Jones and Bartlett, India, New Delhi, 2011.

[4] S. Lang, Complex Analysis, Fourth edition, Addison Wesley, 1999.

Math 301 (ii) – General Measure Theory

Signed measures, complex measures, Hahn decomposition theorem, Jordan decomposition theorem, mutually singular measures. Radon-Nikodym theorem, Lebesgue decomposition, Riesz representation theorem, extension theorem (Caratheodory), Lebesgue-Stieltjes integral, cummulative distribution function, product measures, Fubini's theorem. Tonelli theorem, Differentiation and integration.

Baire sets, Baire measures, continuous functions with compact support, regularity of measures on locally compact spaces, integration of continuous functions with compact support, Riesz · Markov representation theorem.

References:

[1] J.M. G Fell and R. S. Doran, Representation of * - algebras, locally compact groups and Banach *-Algebraic Bundles, Vol I, Academic press Inc , 1988.

[2] P. R. Halmos, Measure Theory, East-West Press Private Ltd., 1978.

[3] E. Hewitt and K.A Ross, Abstract Harmonic Analysis. Vol.I, Springer Verlag, fourth edition, 1993.

[4] H.L. Royden, Real Analysis, Pearson, 2008.

Math 301 (iii) - General Topology

Regularity, complete regularity, the Stone–Čech compactification, normality, Urysohn lemma, Urysohn metrization theorem and Tietze extension theorem, paracompactness, characterizations of paracompactness in regular spaces, Function spaces, topology of point-wise convergence, compact-open topology, exponential law, topologies of uniform convergence, compact convergence and continuous convergence, equicontinuity, Arzela-Ascoli theorem.

References:

[1] J. Dugundji, Topology, Allyn and Bacon, 1970.
[2] R. Engelking, General Topology, Heldermann, 1989.
[3] J.L. Kelley, General Topology, Springer-verlag, 2005.
[4] J.R. Munkres, Topology, Second Edition, Pearson Education, 2003.
[5] S. Willard, General Topology, Dover Publications, Inc. N.Y., 2004.

Math 302 (i) – Fourier Analysis

Convergence and divergence of Fourier series. Fejer's theorem Approximate identities. The classical kernels : [Fejer's, Poisson's and Dirichlet's Summability in norm and pointwise summability], Fatou's Theorem. The inequalities of Hausdorff and Young. Examples of conjugate function series. The Fourier transform. Kernels on R. Basic properties of topological groups, separation properties, subgroups, quotient groups and connected groups. Notion of Haar Measure on topological groups with emphasis on R, T, Z and some simple matrix groups. L^1 (G) and convolution with special emphasis on L^1 (R), L^1 (T), L^1 (Z). Plancherel theorem on abelian groups. Plancherel measure on R, T, Z. Maximal ideal space of L^1(G) (G an abelian topological group).

References:

[1] H. Helson, Harmonic Analysis, Addison-Wesley, 983, Hindustan Pub. Co., 1994.

[2] E. Hewitt and K.A. Ross, Abstract Harmonic Analysis Vol. I, Springer-Verlag, 1993.

[3] Y. Katznelson, Introduction to Harmonic Analysis, John Wiley, 2004.

Math 302(ii) - Matrix Analysis

Closed subgroups of General Linear group. Examples and their compactness and connectedness. Norms for vectors and matrices. Geometric properties of vector norms. Matrix norms. Error in inverses and solution of linear systems. Matrix exponential. Location and perturbation of eigen values. Gersgorin discs. Other inclusion regions.Positive definite matrices. Polar form and singular value decomposition. Applications of singular value decomposition. The schur product theorem. Inequalities for positive definite matrices.Positive matrices and Perron's theorem. Majorisation and Doubly Stochastic Matrices.

References:

1. R. Bhatia, Matrix Analysis, Springer Verlag, 1996
2. B.C.Hall, Lie groups, Lie Algebras, and Representations An Elementary Introduction, Springer Verlag, 2003
3. R.A.Horn and C.R.Johnson, Matrix Analysis, Cambridge University Press, 1994.

Math 302 (iii) – Theory of Operators

Spectrum, Basic concepts, point, continuous and residue spectrum, approximate point spectrum and compression spectrum, spectral mapping theorem for polynomials, Uniform, strong and weak operator convergences on the space of bounded linear operators.

Compact linear operators, properties of compact operators, adjoint of compact operators, Spectral properties of compact operators, Fredholm theory of compact operators and operator equations.

Spectral properties of self-adjoint linear operators, Positive operators and their properties, projection operators and their properties, spectral representation of a self-adjoint compact operator, application to the integral operators, spectral family of self-adjoint operators, spectral representation of a self-adjoint operator, continuous functions of self-adjoint operators, properties of the spectral family of a bounded self-adjoint operator.

Polar decomposition, singular values, trace class operators, trace norm and trace, Hilbert-Schmidt operators.

References

(1) Rajendra Bhatia, Notes on Functional Analysis, Texts and Reading in Mathematics, Hindustan Book Agency (2009).
(2) J. B. Conway, A Course in Functional Analysis, Springer (1990).
(3) Y. Eidelman, V. Milman, A. Tsolomitis, Functional Analysis An Introduction, American Mathematical Society (2004).
(4) E. Kreyszig, Introductory Functional Analysis with Applications, John Wiley and Sons (2001).
(5) P. D. Lax, Functional Analysis, John Wiley and Sons (2002).

Math 302 (iv) -
Computational Methods for Ordinary Differential Equations

Initial Value Problems (IVPs) for the system of ordinary differential equations (ODEs); Difference equations; Numerical Methods; Local truncation errors; Stability analysis; Interval of absolute stability; Convergence and consistency.

Single-step Methods: Taylor series method; Explicit and Implicit Runge-Kutta methods and their stability and convergence analysis; Extrapolation method; Runge-Kutta method for the second order ODEs; Stiff-system of differential equations.

Multi-step Methods: Explicit and Implicit multi-step methods; General linear multi-step methods and their stability and convergence analysis; Adams-Moulton method; Adams-Bashforth method; Nystorm method; Multi-step methods for the second order IVPs.

Boundary Value Problems(BVPs): Two point non-linear BVPs for second order ordinary differential equations; Finite difference methods; Convergence analysis; Difference scheme based on quadrature formula; Difference schemes for linear eigen value problems; Mixed boundary conditions; Finite element methods; Assemble of element equations; Variational formulation of BVPs and their solutions; Galerikin method; Ritz method; Finite element solution of BVPs;

Note: 1. This course consists of two parts:
- (i) Final theory examination carries 70 marks
- (ii) Internal assessment examination carries 30 marks

Note: 2. Use of scientific calculator is allowed in theory examination

Books Recommended:

[1] J.C. Butcher, Numerical Methods for Ordinary Differential Equations, John Wiley & Sons, New York, 2003.

[2] J.D. Lambert, Numerical Methods for Ordinary Differential Systems: The Initial Value Problem, John Wiley and Sons, New York, 1991.

[3] K. Atkinson, W.Han and D.E. Stewart, Numerical Solution of Ordinary Differential Equations, John Wiley, New York, 2009.

Math 303 (i) - Introduction to Algebraic Topology

Homotopic maps, homotopy type, retraction and deformation retract. Fundamental group. Calculation of fundamental groups of n-sphere, n ≥ 1, the cylinder, the torus, and the punctured plane. Applications: the Brouwer fixed-point theorem, the fundamental theorem of algebra, free products, free groups, Seifert–Van Kampen theorem and its applications.

Covering projections, the lifting theorems, relations with the fundamental group, universal covering space. The Borsuk-Ulam theorem, classification of covering spaces.

References:

[1] G.E. Bredon, Geometry and Topology, Springer-Verlag, 2005.

[2] W.S. Massey, A Basic Course in Algebraic Topology, Springer-Verlag, 1991.

[3] J.J. Rotman, An Introduction to Algebraic Topology, Springer-Verlag, 2004.

[4] E.H. Spanier, Algebraic Topology, Springer-Verlag, 1989.

Math 303 (ii) – Advanced Group Theory

Regular, coset and conjugate representations, G-sets and applications, normal series, refinements, composition series, Zassenhaus Lemma, Schreier's theorem on refinements, Jordan-Holder theorem.

Solvable groups, derived series, supersolvable groups, minimal normal subgroups, Hall's theorems, Hall subgroup, p-complements, central series, nilpotent groups, Schur's theorem, Fitting subgroup, Jacobi identity, Three subgroup Lemma, Frattini subgroup, Burnside basis theorem.

Indecomposable groups, group with ascending and descending chain conditions, Fitting's Lemma, Krull-Schmidt theorem, subnormal subgroups, semidirect products, Schur-Zassenhaus lemma, transfer and Burnside normal complement theorem and its consequences.

References:

1. T.W. Hungerford, Algebra, Springer-Verlag, New York, 1981.
2. D.J.S. Robinson, A course in the theory of groups, Springer-Verlag, New York, 1996.
3. J.S. Rose, A course on group theory, Dover Publications, New York, 1994.
4. J.J. Rotman, An Introduction to the Theory of Groups, Springer-Verlag, New York, 1995.
5. M. Suzuki, Group Theory-I, Springer-Verlag, Berlin, 1982.

Math 303 (iv) - Computational Fluid Dynamics

Mathematical description of the physical phenomena. Governing equations-mass, momentum, energy, species. General form of the scalar transport equation, Elliptic, parabolic and hyperbolic equations. Methods for deriving discretization equations by finite difference and finite volume method. Method for solving discretization equations.One-dimensional and two dimensional Diffusion Equation, unsteady diffusion, explicit, implicit and Crank-Nicolson scheme. Two dimensional conduction, accuracy, stability and convergence.

Convection and Diffusion- Steady one-dimensional convection and diffusion, upwind, exponential, hybrid, power, QUICK scheme, Two-dimensional convection-diffusion, accuracy of upwind scheme; false diffusion and dispersion, Boundary conditions. Flow field calculation, pressure-velocity coupling, vorticity-stream function formulation, staggered grid, SIMPLE family of algorithms.

Numerical methods for radiation- Radiation exchange in enclosures composed of diffuse gray surfaces, Finite volume method for radiation.

References

1. John D. Anderson, Computational Fluid Dynamics, *McGraw-Hill*, 1995.
2. D.A. Anderson J.C. Tannehill and Richard H. Pletcher, Computational Fluid Mechanics and Heat Transfer, Taylor and Francis, 1997.
3. Ferziger J H, Peric M, Computational Methods for Fluid dynamics, Spriger, 2001.
4. Suhas V. Patankar, Numerical Heat Transfer and Fluid Flow: Taylor and Francis, 2004.
5. Versteeg, H.K. and Malalasekera,W An introduction to Computational Fluid Dynamics: The Finite volume method, Pearson, 2007.
6. P.S. Ghoshdastidar, Computer Simulation of flow and Heat transfer, Tata-McGrahill Ltd, New Delhi(1998).

Math 304 (i) – Coding Theory

The communication channel, the coding problem, types of codes, block codes, error-detecting and error-correcting codes, linear codes, the Hamming metric, description of linear block codes by matrices, dual codes, standard array, syndrome, step-by-step decoding, modular representation, error-correction capabilities of linear codes, bounds on minimum distance for block codes, Plotkin bound, Hamming sphere packing bound, Varshamov-Gilbert-Sacks bound, bounds for burst-error detecting and correcting codes, important linear block codes, Hamming codes, Golay codes, perfect codes, quasi-perfect codes, Reed-Muller codes, codes derived from Hadamard matrices, product codes, concatenated codes.

References:

[1] Raymond Hill, A First Course in Coding Theory, Oxford University Press, 1990.

[2] W.W. Peterson and E.J. Weldon Jr., Error-Correcting Codes, M.I.T. Press, Cambridge, Massachusetts, 1972.

[3] Man Young Rheo, Error Correcting Coding Theory, McGraw Hill Inc., 1989.

[4] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes, North Holland publishing company, 2006.

Math 304 (ii) -Mathematical Programming

Existence theorems, First order optimality conditions and second order optimality conditions for unconstrained optimization problems, Convex functions, Optimization on convex sets, Separation theorem, Quasiconvex functions, Pseudoconvex functions.

Fritz John and Kuhn Tucker optimality conditions for constrained nonlinear programming problems, Second order optimality conditions for constrained problem, Lagrangian saddle points, Lagrangian duality in convex programming.

Quadratic programming, Wolfe's method as application of Kuhn Tucker conditions, Convex simplex method, Penalty function method.

References

1. O. Güler, **Foundation of Optimization**, Springer, 2010.
2. R.K. Sundaram, **A First Course in Optimization Theory**, Cambridge University Press, 2009.
3. M.S. Bazaraa, H.D. Sherali and C.M. Shetty, **Nonlinear Programming: Theory and Algorithms**, John Wiley & Sons, 2006.

Math 304 (iii) – Graph Theory

Graphs: Vertices of graphs, walks and connectedness, degrees, operations on graphs, blocks, cut-points, bridges and blocks, block graphs and cut-point graphs.

Trees: Elementary properties of trees, centers and centroids, block-cut point trees, independent cycles and co-cycles.

Connectivity and Traversability: Connectivity and line connectivity, Menger's theorems, Eulerian graph, Hamiltonian graphs.

Planarity and Coloring: Planar graphs, outer planar graphs, Kuratowski's theorem, dual graphs, chromatic number, five color theorem.

References:

[1] R. Balakrishnan and K. Ranganathan, A Text Book of Graph Theory, Springer, 2000.
[2] B. Bollobas, Modern Graph Theory, Springer, 2002.
[3] G. Chartrand and L. Lesniak, Graphs and Digraphs, 4th Edit., Chapman & Hall (CRC), 2005.
[4] F. Harary, Graph Theory, Narosa Publishing House, New Delhi, 2001.
[5] R.J. Wilson, Introduction to Graph Theory, 4th Edit., Addison Wesley, 1996.

Math 304 (iv) - Methods of Applied Mathematics

Perturbation methods, regular perturbations, singular perturbations, applications of perturbation methods to fluid mechanics. WKB approximations.

Volterra integral equations, relationship between linear differential equations and Volterra integral equations, resolvent kernel of Volterra integral equation, solution of integral equations by resolvent kernel. The method of successive approximations, convolution type equations. Solutions of integral equations with the aid of Laplace transformation.

Fredholm integral equations, iterated kernels, constructing the resolvent kernel with the aid of iterated kernels. Integral equations with degenerate kernels, characteristic numbers and eigen functions, solution of homogeneous integral equations with degenerate kernel, non homogeneous symmetric equations, Fredholm alternative.

Extrema of functional, the variation of a functional and its properties. Euler's equation and its generalization, sufficient conditions for the extremum of a functional, conditional extremum, moving boundary problems, Ritz method.

Stability and bifurcation: basic ideas and one dimensional problem.

REFERENCES:

1. M. Gelfand and S.V. Fomin, Calculus of variations, Prentice Hall, Inc., 2000.
2. F.B. Hildebrand, Methods of applied mathematics, Dover Publication, 1992.
3. M.L. Krasnov, Problems and exercises integral equations, Mir Publication Moscow, 1971.
4. D. Logan: Applied mathematics: A contemporary approach, John Wiley and Sons, New York, 1997.

Math 401 (i) - Differential Geometry

Graph and level sets, vector fields, the tangent space, surfaces, orientation, the Gauss map, geodesics, parallel transport, the Weingarten map, curvature of plane curves, arc length and line integrals, curvature of surfaces, parametrized surfaces, surface area and volume, surfaces with boundary, the Gauss-Bonnet Theorem.

References

[1] Wolfgang Kuhnel: Differential Geometry – curves-surfaces-Manifolds. Second Edition, 2006, AMS.

[2] A: Mishchenko and A. Formentko. A course of Differential Geometry
and topology) Mir Publishers Moscow, 1988.

[3] Andrew Pressley: Elementary Differential Geometry. SUMS (Springer), 2001 (Ist Indian Repring 2004).

[4] I.A. Thorpe: Elementary Topics in Differential Geometry. Springer, 1979 (Ist Indian Reprint 2004).

Math 401(ii) -Commutative Algebra

Extension and Contraction of ideals, Prime spectrum of Rings, Jacobson radical of a ring, Prime avoidance lemma, Rings of formal power series, Restriction and extension of scalars.

Localisation, Local properties, Extended & contracted ideals in rings of fractions, Primary decomposition, First and second uniqueness theorem of primary decomposition, Chain conditions, Noetherian rings, Hilbert's Basis Theorem, Primary decomposition in Noetherian rings, Artin rings, Structure theorem for Artin rings.

Integral dependence, Going up theorem, Going down theorem, Integrally closed domains, Valuation rings, Hilbert's Nullstellensatz theorem, Discrete valuation rings, Dedekind domains, Fractional ideals.

References:

[1] M.F. Athiya & I.G. Macdonald, Introduction to Commutative Algebra, Addison Wesley, 1969.

[2] Balwant Singh, Basic Commutative Algebra, World Scientific Publishing Co., 2011.

[3] D. Eisenbud, Commutative Algebra with a view towards algebraic geometry, Springer Verlag, 1995.

[4] O. Zariski & P. Samuel, Commutative Algebra, Vol. 1 & 2, Springer-Verlag, 1975.

[5] R.Y. Sharp, Steps in Commutative Algebra, Cambridge University Press, 1990

Math-401(iii) - Calculus on $\mathbb{R}^n$

Thedifferentiability of functions from R^ntoR^n, directional derivatives and differentiability, chain rule, inverse function theorem and implicit function theorem.

Integration over a k-cell, primitive mappings, partition of unity, change of variables, Introduction to differential forms on R^n, basic properties of differential forms, differentiation of differential forms, change of variables in differential forms, simplexes and chains, integration of differential forms, Stokes' theorem.

References:

[1]. J.R. Munkres, Analysis on manifolds, Addison Wesley, 1991.

[2]W. Rudin, Principles of Mathematical Analysis, 3rd edition, McGraw Hill, 1986

[2].M. Spivak, Calculus on Manifolds: A Modern Approach to Classical Theorems Of Advanced Calculus, Westview Press, 1998.

Math 402 (i) - Abstract Harmonic Analysis

Introduction to representation theory of involutive Banach algebra. Unitary representation of locally compact groups, Gelfand-Rajkov theorem.

Representation of some special groups SU(2), Lorentz group, the group of linear transformations of the real line. Unitary representation of compact groups. Schur's lemma, the orthogonality relations.

Characters of finite dimensional representation. Weyl-Peter theorem, convolution of bounded regular complex measures.

The convolutive Banach algebra M(G). Fourier-Stieltjes transform. Positive definite functions. Bochner's theorem.

References:

[1] J.M.G. Fell and R.S. Doran, Representation of * Algebras. Locally compact Groups I and Banach* Algebraic Bundles. Vol. I, II, Academic Press Inc., 1988.

[2] E. Hewitt and K.A. Ross, Abstract Harmonic Analysis, Vol. I., II Springer Verlag, 1993.

[3] W. Rudin, Fourier Analysis on Groups, Interscience Publisher, 1990.

Math 402 (ii) - Advanced Functional Analysis

Introduction to topological vector spaces and locally convex spaces, linear operators, uniform boundedness principle, closed graph theorem, open mapping theorem, Hahn-Banach theorem, extreme points and Krein-Milman theorem.

Geometry of Banach spaces: vector measures, Radon-Nikodym property and geometric equivalents, Choquet theory. Weak compactness and Eberlein-Smulian theorem, Schauder basis.

References:

[1] J. Diestel and J. J. Uhl, Jr., Vector measures. Mathematical Surveys, No. 15. American Mathematical Society, 1998.

[2] N. Dunford and J. T. Schwartz, Linear operators. Part II: Spectral theory. Self adjoint operators in Hilbert space. Interscience Publishers John Wiley & Sons, 1963.

[3] Walter Rudin, Functional analysis. International Series in Pure and Applied Mathematics. McGraw-Hill, Inc., 1991.

[4] K. Yosida, Functional analysis. Grundlehren der Mathematischen Wissenschaften, 123. Springer-Verlag, 2008.

Math. 402(iii)-Theory of Frames

Haar Wavelet Analysis: Haar Wavelets, Basic properties of the Haar scaling function, Haar decomposition and reconstruction algorithms, Filter and Diagrams. Comparison of Haar series with Fourier series.

Multiresolution Analysis: The Scaling Relation, The associated wavelet and wavelet spaces, Decomposition and reconstruction formulas, The decomposition and reconstruction algorithm, Processing a signal. Fourier Transform Criteria.

Frames: Bessel sequences in Hilbert spaces, Riesz bases, The Gram matrix, Gabor bases,Frames and their properties, Frame sequence, Frames and Riesz bases, Bases in Banach spaces, Limitations of bases, Frames and operators, Frames and bases, Characterization of frames, The dual frames, Tight frames, Continuous frames, frames and signal processing. Conditions for a frame being a Reisz basis, Frames contaiing a Riesz basis, Frames which does not contain a basis, Comparison between frames and Riesz bases. Frames in finite dimensional Hilbert spaces.

Wavelet versus frames: Wavelets frames and wavelet sets, Estimates of wavelet frame bounds, Admissibility Condition, Signal and Systems, Perturbation of wavelet frame.

References

[1] Ole Christensen, *An introduction to frames and Riesz bases*, *Birkhäuser* (2003)

[2] Ole Christensen, *Frames and bases* , *Birkhäuser*(2008)

[3] Christopher Heil, *A Basis Theory Primer* (Expanded Edition), *Birkhäuser* (2011)

[4] K. Grochenig, *Foundations of time- frequency analysis*, *Birkhäuser* (2000).

[5] Albert Boggess and Francis J. Narcowich, *A first course in wavelets and Fourier analysis*, *Wiley* (2009)

[6] David F. Walnut, *An Introduction to Wavelet Analysis*, *Birkhäuser* (2002).

Math 402 (iv) - Operators on the Hardy-Hilbert Space

The Hardy-Hilbert Space: Basic definitions and properties.

The unilateral shift and factorization of functions: Shift operators. Invariant and reducing subspaces. Inner and outer factorization. Balschke factors. Singylar inner functions. Outer functions.

Toeplitz operators: Basic properties of Toeplitz operators. Spectral structure.

Hankel operators: Bounded Hankel operators. Hankel operators of finite rank. Compact Hankel operators. Self adjointedness and normality of Hankel operators. Relation between Hankel and Toeplitz operators.

References:

[1] R. G. Douglas, Banach Algebra Techniques in Operator Theory, Graduate Texts in Mathematics 179, Springer, 1998.

[2] R.A. Martinez-Avedano & P. Rosenthal, An Introduction to the Hardy-Hilbert Space, Graduate Texts in Mathematics 237, Springer, 2007.

[3] N. K. Nikolskii, Operators, Functions and Systems: An Easy Reading, Volume I, Mathematical Surveys and Monographs 92, American Mathematical Society, 2002.

Math 402 (v)-
Computational Methods for Partial Differential Equations

Finite difference methods for 2D and 3D elliptic boundary value problems (BVPs) of second and fourth order approximations; Finite difference approximations to Poissons equation in cylindrical and spherical polar coordinates; Solution of large system of algebraic equations corresponding to discrete problems and iterative methods (Jacobi, Gauss-Seidel and SOR); Alternating direction methods.

Different 2- and 3-level explicit and implicit finite difference approximations to heat conduction equation; Stability analysis (Energy method, Matrix method and Von-Neumann method); Compatibility, consistency and convergence of the difference methods; Difference scheme based on derivative boundary conditions and its stability condition; ADI methods for 2- & 3-D parabolic equations; Finite difference approximations to heat equation in polar coordinates.

Methods of characteristics for evolution problem of hyperbolic type; Von-Neumann method for stability analysis; Operator splitting methods for 2D and 3D wave equations; Explicit and implicit difference schemes for first order hyperbolic equations and their stability analysis; System of equations for first order hyperbolic equations; Conservative form.

Finite element methods for second order elliptic BVPs; Finite element equations; Variational problems; Triangular and rectangular finite elements; Standard examples of finite elements; Mixed finite element methods.

Note: 1. This course consists of two parts:

(i) Final theory examination carries 70 marks
(ii) Internal assessment examination carries 30 marks

Note: 2. Use of scientific calculator is allowed in theory examination

Books Recommended:

[1] J.C. Strickwerda, Finite Difference Schemes & Partial Differential Equations, SIAM publications, 2004.

[2] J.W.Thomas, Numerical Partial Differential Equations: Finite Difference Methods, Springer and Verlag, Berlin, 1998.

[3] J.W.Thomas, Numerical Partial Differential Equations: Conservation Laws and Elliptic Equations, Springer and Verlag, Berlin, 1999.

Math 403 (i) - Homology Theory

Geometric simplexes, geometric complexes and polyhedra. Simplicial maps, barycentric subdivision, simplicial approximation of continuous maps, contiguous maps, abstract simplicial complex.

Orientation of geometric complexes, homology groups. Computation of homology groups, the homology of n-sphere, $n \geq 1$. The structure of homology groups, the chain complexes, chain mappings, chain derivation, chain homotopy. The homomorphism induced by continuous maps between two polyhedra.

Singular complex and homology groups, functorial properties, the Eilenberg-Steenrod axioms of homology theory. The reduced homology groups, the Mayer-Vietoris sequence. The degree of self mappings of S^n, the Brouwer's fixed point theorem, the Euler-Poincaré theorem and Lefschetz fixed point theorem.

References:

[1] H. Agoston, Algebraic Topology, Marcel Dekker, 1976.
[2] M. A. Armstrong, Basic Topology, Springer-Verlag, 1983.
[3] F.H. Croom, Basic Concepts of Algebraic Topology, 1976.
[4] A. Dold, Lectures on Algebraic Topology, Springer-Verlaq, second edition, 1980.
[5] J.J. Rotman, An Introduction to Algebraic Topology, Springer-Verlag, 1988.

Math 403 (ii) - Theory of Noncommutative Rings

Basic terminology and examples, semisimplicity, structure of semisimple rings, Wedderburn–Artin's theorem, Jacobson radical, prime radical, prime and semiprime rings, structure of primitive rings, density theorem, direct products, subdirect sums, commutativity theorems and local rings

References:

[1] I.N. Herstein, A First Course in Noncommutative Rings, Carus Monographs of AMS 1968.

[2] Louis H. Rowen, Ring Theory, Academic Press, 1991.

[3] T.W. Hungerford, Algebra, Springer Verlag, New York, 1981.

[4] T.Y. Lam, A first course on Non-Commutative Rings, Springer-Verlag, 1991.

Math 403 (iii) – Algebraic Number Theory

Algebraic numbers, number fields, conjugates and discriminants, algebraic integers, integral bases, norms and traces, rings of integers, quadratic fields and cyclotomic fields.

Trivial factorizations, factorization into irreducibles, examples of non-unique factorization into irreducibles, prime factorization, Euclidean domains and Euclidean quadratic fields, consequences of unique factorization, the Ramanujan-Nagell theorem. Prime factorization of ideals, norm of an ideal, non-unique factorization in cyclotomic fields

Lattices of dimension *m*, the quotient torus, Minkowski's theorem, two-squares theorem, four-squares theorem, the space L^{st}. The class-group, finiteness of the class-group, unique factorization of elements in an extension ring, factorization of a rational prime, Minkowski's constants, class-number calculations.

References:

[1] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, 1990.

[2] S. Lang, Algebraic Number Theory, Springer-Verlag, New York Inc., 1994.

[3] D.A. Marcus, Number Fields, Springer-Verlag, New York Inc., 1987.

[4] I. N. Stewart and D. O. Tall, Algebraic Number Theory, Chapman and Hall, London, 1987.

Math 403 (iv)- Advanced Fluid Mechanics

Thermodynamics: Equation of state of a substance, First law of Thermodynamics, Internal energy and specific heat of gas, entropy, Second law of thermodynamics.

Physical similarity and Dimensional Analysis: Types of physical similarity, Nondimensionalizing the basic equation of incompressible viscous fluid flow, non-dimensional parameters, Dimensional analysis and Buckingham Pi Theorem.

Gas Dynamics: Compressibility effects, Elements of wave motion in a gas, Speed of sound, Basic equation of one-dimensional compressible flow, Subsonic, sonic and supersonic flows, Isentropic gas Flow, Flow through a nozzle, Normal shock wave, oblique shock wave and their elementary analysis.

Magnetohydrodynamics: Concept, Maxwell' electromagnetic field equations, Equation of motion of a conducting fluid, MHD approximations, Rate of flow of charge, Magnetic Reynolds number and Magnetic field equation, Alfven's theorem, Magnetic body force, Ferraro's Law of isorotation.

Boundary Layer theory: Concept, Boundary layer thickness, Prandtl's boundary layer, Boundary layer on flat plate: Blassius solution, Karman's integral equation.

References

1. Text Book of Fluid Dynamics, F. Chorlton, GK Publisher,2009
2. Fluid Mechanics, P.K.Kundu, I.M.Cohen, Academic Press,2010
3. Introduction to Fluid Mechanics, R.W.Fox, P.J.Pritchard, A.T.Mcdonald. John Wiley and Sons, 2010
4. Introduction to Fluid Mecanics, G.K.Batchelor, Foundation book, New Delhi. 1994
5. Compressible Fluid Flow, S.I.Pai, New York, Ronald Press, 1954
6. Alan Jeffery, Magnetohydrodynamics, Oliver and Boyd Ltd., Edinburgh, 1966

Math 404 (i) – Advanced Coding Theory

Tree codes, convolutional codes, description of linear tree and convolutional codes by matrices, standard array, bounds on minimum distance for convolutional codes, V-G-S bound, bounds for burst-error detecting and correcting convolutional codes. The Lee metric, packing bound for Hamming code w.r.t. Lee metric. The algebra of polynomials, residue classes, Galois fields, multiplicative group of a Galois field, cyclic codes, cyclic codes as ideals, matrix description of cyclic codes, Hamming and Golay codes as cyclic codes, error detection with cyclic codes, error-correction procedure for short cyclic codes, shortended cyclic codes, pseudo cyclic codes, code symmetry, invariance of codes under transitive group of permutations, Bose-Chaudhary-Hocquenghem (BCH) codes, BCH bounds, Reed-Solomon (RS) codes, majority-logic decodable codes, majority-logic decoding, singleton bound. The Griesmer bound, maximum-distance separable (MDS) codes, generator and parity-check matrices of MDS codes, weight distribution of MDS code, necessary and sufficient conditions for a linear code to be an MDS code, MDS codes from RS codes, Abramson codes, closed-loop burst-error correcting codes (Fire codes), error locating codes.

References:

[1] E.R. Berlekamp, Algebraic Coding Theory, McGraw Hill Inc., 1984..

[2] W.C. Huffman and V. Pless, The Theory of Error Correcting Codes, Cambridge University Press, 1998.

[3] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes, North Holland publishing company, 2006.

[4] W.W. Peterson and E.J. Weldon Jr., Error-Correcting Codes, M.I.T. Press, Cambridge, Massachusetts, 1972.

Math 404 (ii)-Optimization Techniques and Control Theory

Functions taking values in extended reals, Proper convex functions, Subgradients, Directional derivative, Conjugate functions, Conjugate duality.

Gradient descent method, Gradient projection method, Newton's method, Conjugate gradient method.

Dynamic programming, Bellman's principle of optimality, Allocation problem, Cargo load problem, Stage coach problem.

Optimal control problem, Classical approach to solve variational problem, Pontryagin's maximum principle, Dynamic programming and maximum principle.

References

1. M. Avriel, **Nonlinear Programming: Analysis and Methods**, Dover Publications, New York, 2003.
2. O. Güler, **Foundation of Optimization**, Springer, 2010.
3. F. Hillier, G.J. Lieberman, **Introduction to Operations Research**, McGraw-Hill College, 2009.
4. D. Liberzon, **Calculus of Variations and Optimal Control Theory: A Concise Introduction**, Princeton University Press, 2012.

Math 404 (iii) – Cryptography

Secure communications, shift ciphers, affine ciphers, vigenere cipher key, symmetric key, public key, block ciphers, one time pads, secure random bit generator, linear feedback shift register sequences.

Differential cryptanalysis, modes of DES, attack on DES, advanced encryption standard.

RSA, attack on RSA, Diffie-Hellman key exchange, ElGamal public key cryptosystem, cryptographic hash function, RSA signatures, ElGamal signature, hashing and signing, digital signature algorithm.

References:

[1] Johannes A Buchmann, Introduction to Cryptography, Springer, 2000.

[2] Douglas Robert Stinson, Cryptography – Theory and Practice, Chapman Hall (CRC), 2006.

[3] Wade Trappe and Lawrence C Washington, Introduction to Cryptography with Coding Theory, Pearson Prentice Hall, 2006.