Program Outcomes for Science Doctoral Program

1. **In-depth Knowledge:** Acquire basic in-depth and advance knowledge by critically applying and comprehensive understanding of methodologies to address issue and question of a science discipline and attain specialization in a particular domain.

2. **Research and Scientific Reasoning:** Apply theories, methodologies, knowledge, critical thinking and inductive and deductive reasoning to design and drive research projects with appropriate hypothesis, experimental design, simulation, etc.

3. **Communication and Digital Skills**: Acquire proficiency in oral and written communication skills to comprehend and write effective reports, design documents, make effective presentation, and give and receive clear instructions,

4. **Professional Ethics:** Acquire the knowledge of ethics and values to inculcate fair practices throughout their professional life.

5. **Project Management:** Develop and apply knowledge of science and technology, project management and finance principles, in a multidisciplinary setting, to carry out meaningful research and project work.

6. **Leadership Readiness**: Interact with people from diverse backgrounds as both leaders/mentors and team members with integrity and professionalism.

Program Specific Outcomes for Doctoral Programme in Mathematics:

The PSOs of the Doctoral program in Mathematics are as follows:

PSO1: Generate publications in reputed mathematical journals.

PSO2: Provide scope for interaction with international researchers and developing collaborations.

PSO3. Developing knowledge of the literature and a comprehensive understanding of scientific methods and techniques applicable to their own research.

PSO4. Provide opportunities to research students for communication (and discussion) of advanced mathematical topics to undergraduate and graduate students.

O P JINDAL UNIVERSITY

O P Jindal Knowledge Park, Punjipathra, Raigarh-496109

School of Science, Department of Mathematics

UNIVERSITY OF STEEL TECHNOLOGY AND MANAGEMENT

Programme:	**PhD(Course Work)**	**Semester :**	
Name of the Course:	**Advanced Numerical Analysis**	**Course Code:**	**PMA 102**
Credits :	**5**	**No of Hours :**	**50**
Max Marks:	**100**		

Course Description:

The objective of the course is to familiarize the students about some advanced numerical techniques e.g. solving systems of nonlinear equations, linear system of equations, Eigen value problems, Interpolation and Approximation techniques and their use in differentiation and integration, differential equations etc.

COURSE OUTCOMES:

On successful completion of this course, students will be able to:

CO Number	Course Outcome
CO1	Understand methods for multiple roots, Muller's, Iteration and Newton-Raphson method for non-linear system of equations, and Newton-Raphson method for complex roots.
CO2	Understand Descartes' rule of signs, Birge-Vieta, Bairstow and Giraffe's methods. System of Linear Equations: Triangularization, Cholesky and Partition methods, SOR method .
CO3	Understand Similarity transformations, Gerschgorin's bound(s) on eigenvalues, Givens, Householder and Rutishauser methods.
CO4	Understand Spline and bivariate interpolation, Gram-Schmidt orthogonalisation, Legendre and Chebyshev polynomials and approximation.
CO5	Determine continuity at a point or on intervals and distinguish between the types of discontinuities at a point.
CO6	Understand shooting and finite difference methods for second order boundary value problems, Applications of cubic spline to ordinary differential equation of boundary value type.
CO7	Understand Finite difference methods for Elliptic, Parabolic and Hyperbolic partial differential equations

CO8	Understand basic concepts of the calculus of variations such as functionals, extremum, variations, function spaces, the brachistochrone problem
CO9	Understand Variational derivative. Invariance of Euler`s equations
CO10	Understand Variational problem in parametric form, Rayleigh-Ritz method, Galerkin's method.

Syllabus:

UNIT- I

Non-Linear Equations: Methods for multiple roots, Muller's, Iteration and Newton-Raphson method for non-linear system of equations, and Newton-Raphson method for complex roots. Polynomial Equations: Descartes' rule of signs, Birge-Vieta, Bairstow and Giraffe's methods. System of Linear Equations: Triangularization, Cholesky and Partition methods, SOR method with optimal relaxation parameters.

UNIT-II

Eigen-Values of Real Symmetric Matrix: Similarity transformations, Gerschgorin's bound(s) on eigenvalues, Givens, Householder and Rutishauser methods.

Interpolation and Approximation: B - Spline and bivariate interpolation, Gram-Schmidt orthogonalisation process and approximation by orthogonal polynomial, Legendre and Chebyshev polynomials and approximation.

UNIT- III

Differentiation and Integration: Differentiation and integration using cubic splines, Romberg integration and multiple integrals.

Ordinary Differential Equations: Shooting and finite difference methods for second order boundary value problems, Applications of cubic spline to ordinary differential equation of boundary value type.

UNIT- IV

Partial Differential Equations: Finite difference methods for Elliptic, Parabolic and Hyperbolic partial differential equations.

UNIT- V

Calculus of Variation: Basic concepts of the calculus of variations such as functionals, extremum, variations, function spaces, the brachistochrone problem. Necessary condition for an extremum, Euler`s equation with the cases of one variable and several variables, Variational derivative. Invariance of Euler`s equations. Variational problem in parametric form, Rayleigh-Ritz method, Galerkin's method,

Reference Books:

1. K. Atkinson, *An Introduction to Numerical Analysis*, John Wiley & Sons, 2nd Edition, 1989.
2. R. L. Burden and J. D. Faires, *Numerical Analysis*, 9th Edition, Cengage Learning, 2011.
3. S. D. Conte, S.D. and Carl D. Boor, *Elementary Numerical Analysis: An Algorithmic* Approach, Tata McGraw Hill 2005.
4. C. F. Gerald and P. O. Wheatly, *Applied Numerical Analysis*, 7th Edition, Pearson LPE, 2009.
5. R. S. Gupta, *Elements of Numerical Analysis*, Cambridge University Press, 2nd Edition, 2015.
6. M. K. Jain, S.R.K. Iyengar and R.K. Jain, *Numerical Methods for Scientific and Engineering Computation*, 6th Edition, New Age International, New Delhi, 2015.

CO-PO&PSO Correlation

Course Name : Advanced Numerical Analysis										
	Program Outcomes						**PSOs**			
Course	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**
CO1:	**2**						**3**			
CO2:		**1**						**2**		
CO3:			**3**				**1**			
CO4:		**2**		**1**						**1**
CO5:	**1**		**2**					**1**		
CO6:		**1**					**1**			
CO7:	**1**				**1**			**1**		
CO8:			**2**						**2**	
CO9:			**1**				**1**			
CO10:		**1**				**2**		**1**		

Note: 1: Low 2: Moderate 3: High

O P JINDAL UNIVERSITY

O P Jindal Knowledge Park, Punjipathra, Raigarh-496109

School of Science, Department of Mathematics

OPJU
UNIVERSITY OF STEEL TECHNOLOGY AND MANAGEMENT

Programme:	**PhD(Course Work)**	**Semester :**	
Name of the Course:	**Magnetohydrodynamics**	**Course Code:**	**PMA 104**
Credits :	**5**	**No of Hours :**	**50**
Max Marks:	**100**		

Course Description:

Introduction to Magnetohydrodynamics (MHD) course has been designed for students who are familiar with basics of electromagnetic theory and vector calculus. MHD is essentially an extension of hydrodynamics to electrodynamics. In this course, the theoretical basis for and regime of validity of ideal and resistive magnetohydrodynamics (MHD) is presented. Magnetohydrodynamics, or MHD for short, is concerned with understanding the nature of fluid flows in the presence of magnetic fields. It therefore combines electromagnetic theory with fluid dynamics. This course gives a basic introduction to MHD, detailing how magnetic fields can have significant effects on the nature of fluid flows (including the important topic of plasma confinement in fusion devices) and how fluid flows can self-consistently lead to the generation of magnetic fields.

COURSE OUTCOMES:

On successful completion of this course, students will be able to:

CO Number	Course Outcome
CO1	Understand the concept of rotational and irrotational flow, stream functions, velocity potential, sink, source, vortex etc
CO2	Analyze simple fluid flow problems (flow between parallel plates, flow through pipe etc.) with Navier-Stoke's equation of motion
CO3	Understanding the electromagnetic induction mechanism which has its origin in the movement of fluids that are good electrical conductors and phenomenon of flow separation and boundary layer theory.
CO4	Able to translate a magnetic hydrodynamic problem in an appropriate mathematical form
CO5	Students can interpret the solutions of the equations established in physical terms. Understand the concept of thermal conductivity.

CO6	Understand the basic concepts and the equations of flow of viscous fluids learn about the fundamental equations of the flow and energy
CO7	Understand Alfven's theorem, Alfven's wave, Magnetic energy, Dissipative effect, Plane polarized waves.
CO8	Understand MHD waves in compressible fluid, Electromagnetic boundary conditions.
CO9	Understand MHD channel Flows, MHD Stokes flow, MHD Rayleigh's Flow.
CO10	Understand MHD Flow in Rotating Medium, MHD Heat Transfer

Syllabus:

Basic concepts of Magneto-hydrodynamics, Lorentz force, Frame of reference, Electromagnetic Body force, Fundamental equations of MHD, Derivation of magnetic induction equation, Ohm's law for a moving conductor, Hall and Conduction currents, Kinematic aspects of MHD. Electromagnetic Radiation, Magnetic Pressure, pointing vector, Alfven's theorem, Alfven's wave, Magnetic energy, Dissipative effect, Plane polarized waves, MHD waves in compressible fluid, Electromagnetic boundary conditions, One-dimensional flows: MHD channel Flows, MHD Stokes flow, MHD Rayleigh's Flow, MHD Flow in Rotating Medium, MHD Heat Transfer.

Reference Books:

1. P. A. Davidson, *An Introduction to Magnetohydrodynamics*, Cambridge University Press.
2. T.G. Cowling, *Magnetohydrodynamics*, Interscience tracts on physics and astronomy.
3. J. A. Shercliff, *A Textbook of Magnetohydrodynamics*, Cambridge.
4. P.H. Roberts, *An Introduction to Magnetohydrodynamics*, 1967, Longman.
5. Arthur Sherman and George Walter Sutton, *Engineering Magnetohydrodynamics*, Dover.
6. Fred J. Young, William F. Hughes, *The Electromagnetodynamics of Fluids.*
7. Hosking, Roger J., Dewar, Robert, *Fundamental Fluid Mechanics and magnetohydrodynamics*, Springer.
8. Lorrain, Paul, Lorrain, Francois, Houle, Stephane, *Magneto-Fluid Dynamics (Fundamentals and Case Studies of Natural Phenomena).*

O P JINDAL UNIVERSITY

O P Jindal Knowledge Park, Punjipathra, Raigarh-496109

School of Science, Department of Mathematics

CO-PO&PSO Correlation

Course Name : Magnetohydrodyanamics										
	Program Outcomes						PSOs			
Course	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**
CO1:		2					3			
CO2:	1							2		
CO3:			2				2			
CO4:		2		3						1
CO5:	2		3					3		
CO6:		2					1			
CO7:	1				1			1		
CO8:		3							2	
CO9:			1				3			
CO10:		1				1		2		

Note: 1: Low 2: Moderate 3: High

Programme:	**PhD(Course Work)**	**Semester :**	
Name of the Course:	**Real Analysis and Complex Analysis**	**Course Code:**	**PMA 105**
Credits :	**5**	**No of Hours :**	**50**
Max Marks:	**100**		

Course Description:

This course covers the fundamentals of mathematical analysis: convergence of sequences and series, continuity, differentiability, Riemann integral, sequences and series of functions, uniformity, and the interchange of limit operations**.** The course studies complex integration, conformal maps, harmonic and subharmonic functions, Dirichlets problem, series and product expansions, elliptic functions, and analytical continuation.

COURSE OUTCOMES:

On successful completion of this course, students will be able to:

CO Number	Course Outcome
CO1	Explain Continuity and Discontinuity of various functions in different contexts
CO2	Differentiate Uniform continuity from continuity and related theorems
CO3	Understand the meaning of derivative of a function
CO4	Acquire skill in applying the various techniques of differentiation and applications
CO5	Explain convergence of a series and illustrate the convergence properties of power series
CO6	Understand Casorati- Weierstrass therorem, Bloch-Landau therorem, Picard's therorems, Mobius transformations, Schwarz lemma
CO7	Understand External metrics, Riemann mapping theorem, Argument

	principle, Rouche's theorem.
CO8	Understand Runge's theorem, Infinite products, Weierstrass p-function, Mittag-Leffler expansion.
CO9	Understand linear transformation, Differentiation, The contraction principle, The inverse Function Theorem.
CO10	Understand The Implicit Function Theorem, Derivative of Higher orders, Langrage's Multiplier Method.

Syllabus:

Unit I

Sequences and series, convergence, limsup, liminf. Bolzano Weierstrass theorem, Continuity, uniform continuity, differentiability, mean value theorem. Uniform convergence. Riemann-Stieltjes Integral: Definition and Existence of Integral, Properties of Integral, Integration and Differentiation, Improper integral, Integration of Vector-valued functions, Monotonic functions, types of discontinuity, functions of bounded variation.

Unit II

Function of Several Variables: Linear transformation, Differentiation, The contraction principle, The inverse Function Theorem, The Implicit Function Theorem, Derivative of Higher orders, Langrage's Multiplier Method.

Unit III

Analytic functions, Path integrals, Winding number, Cauchy integral formula and consequences. Gap theorem, Isolated singularities, Residue theorem, Liouville theorem.

Unit IV

Casorati- Weierstrass therorem, Bloch-Landau therorem, Picard's therorems, Mobius transformations, Schwartz lemma, External metrics, Riemann mapping theorem, Argument principle, Rouche's therorem..

Unit V

Runge's theorem, Infinite products, Weierstrass p-function, Mittag-Leffler expansion.

Reference Books:

1. S. C. Malik, S. Arora, Mathematical Analysis, New Age International.

2. Walter Rudin Principle of Mathematical Analysis, McGraw-Hill.
3. L. V. Ahlfors, Complex Analysis, McGraw-Hill, Inc., 1996.
4. A. R. Shastri, Complex Analysis, 2010.
5. S. G. Krantz, Complex Analysis: The Geometric View Points, Second edition, Carus Math. Monographs, MAA.
6. T. Apostol, Mathematical Analysis, Narosa Publishers.
7. H. L. Roydon, Real Analysis, Macmillan Publication, New York
8. K. Ross, Elementary Analysis: The Theory of Calculus, Springer.
9. R.V. Churchill and Brown, Complex variables and applications, McGraw Hill.
10. S. Ponnusamy, Foundations of Complex Analysis, Narosa Publishing House.
11. Murray Speigel, Complex Variables, Shaum's Outline Series
12. Walter Rudin, Real and Complex Analysis, McGraw-Hill Book Co.
13. S. Lang, Complex Analysis, Addison Wesley.

CO-PO&PSO Correlation

Course Name : Real Analysis and Complex Analysis										
	Program Outcomes						**PSOs**			
Course	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**
CO1:		2					1			
CO2:	2							2		
CO3:			3				2			
CO4:		2		1						3
CO5:	1		2					1		
CO6:		1					2			
CO7:	1				1			1		
CO8:		2							2	
CO9:			3				3			
CO10:		1				1		1		

Note: 1: Low 2: Moderate 3: High

Programme:	**PhD(Course Work)**	**Semester :**	
Name of the Course:	**Geometric Function Theory**	**Course Code:**	**PMA 106**
Credits :	**5**	**No of Hours :**	**50**
Max Marks:	**100**		

Course Description:

Geometric function theory is a branch of complex analysis that seeks to relate analytic properties of conformal maps to geometric properties of their images. The subject has deep connections with other areas of mathematics such as potential theory, hyperbolic geometry, and dynamical systems. The course aims to introduce students to geometric function theory in a broad sense, and to define concepts and present techniques required in modern applications such as the theory of the Schramm-Loewner evolution.

COURSE OUTCOMES:

On successful completion of this course, students will be able to:

CO Number	Course Outcome
CO1	Understand basics of Geometric function Theory
CO2	Understand Area theorem, growth, distortion theorems, coefficient estimates for univalent functions.
CO3	Understand special classes(Starlile, Convex, Close to Convex,…) of univalent functions
CO4	Understand Lowner's theorem and its applications.
CO5	Understand de Banges proof of Bieberbach conjecture and generalization of the area theorem, Grunsky inequalities.
CO6	Understand exponentiation of the Grunsky inequalities, Logarithmic coefficients.
CO7	Understand Subordination and Sharpened form of Schwarz Lemma References.

CO8	Understand Superordination and its applications

Syllabus:

Unit 1: Area theorem, growth, distortion theorems, coefficient estimates for univalent functions special classes of univalent functions. Lowner's theory and its applications; outline of de Banges proof of Bieberbach conjecture.

Unit 2: Generalization of the area theorem, Grunsky inequalities, exponentiation of the Grunsky inequalities, Logarithmic coefficients.

Unit 3: Subordination and Sharpened form of Schwarz Lemma References.

Unit 4: Superordination and its applications.

Reference Books:

1. P. Duren, Univalent Functions, Springer, New York, 1983
2. A. W. Goodman, Univalent Functions I & II, Mariner, Florida, 1983
3. Ch. Pommerenke, Univalent Functions, Van den Hoek and Ruprecht, Göttingen, 1975.
4. M. Rosenblum, J. Rovnyak, Topics in Hardy Classes and Univalent Functions, Birkhauser Verlag, 1994.
5. D. J. Hallenbeck, T. H. MacGregor, Linear Problems and Convexity Techniques in Geometric Function Theory, Pitman Adv. Publ. Program, Boston-London-Melbourne,1984.
6. I.Graham, G. Kohr, Geometric Function Theory in One and Higher Dimensions, Marcel Dekker, New York, 2003.

CO-PO&PSO Correlation

Course Name : Geometric Function Theory										
	Program Outcomes						**PSOs**			
Course	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**
CO1:		**1**					**1**			
CO2:	**2**							**3**		
CO3:			**3**				**2**			
CO4:		**2**		**1**						**1**
CO5:	**1**		**3**					**1**		
CO6:		**1**					**1**			
CO7:	**1**				**1**			**1**		
CO8:		**2**							**2**	

Note: 1: Low 2: Moderate 3: High

O P JINDAL UNIVERSITY

O P Jindal Knowledge Park, Punjipathra, Raigarh-496109

School of Science, Department of Mathematics

OPJU
UNIVERSITY OF STEEL TECHNOLOGY AND MANAGEMENT

Programme:	**PhD(Course Work)**	**Semester :**	
Name of the Course:	**Number Theory**	**Course Code:**	**PMA 107**
Credits :	**5**	**No of Hours :**	**50**
Max Marks:	**100**		

Course Description:

This course is an introduction to the fundamentals of number theory, with a survey of additional topics that are accessible once the basics are in place. The course is intended to introduce concepts of number theory from a rigorous point of view, and then show students some of the applications of the material they have just learned. Not as deep as, as but generally broader as a one-semester course for math majors at universities. The course is core material: axioms for the number system, divisibility and the GCD, factorization, Euclidean algorithm, linear Diophantine equations, the multiplicative functions sum and number of divisors. Congruences, systems and the Chinese Remainder Theorem, reduced residue systems and Euler's totient function. Euler and Fermat theorems, primality testing, order and primitive roots. Representations of numbers in base *b*, periodic expansions, irrational numbers and cardinality.

COURSE OUTCOMES:

On successful completion of this course, students will be able to:

CO Number	**Course Outcome**
CO1	Understand Primes, Divisibility, primality testing and factorization methods.
CO2	Understand Euclidean Algorithm, Extended Euclidean algorithm.
CO3	Acquire the concept of Congruences, Ring of Integers mod n, Chinese Remainder Theorem and understand arithmetic Functions, Fermat's little theorem, Primitive roots
CO4	Understand Mobius Inversion formula, properties of Mobius function.
CO5	Acquire the concept of recurrence functions, Fibonacci numbers and their elementary properties
CO6	Understand Quadratic Residues, Quadratic Reciprocity Law, Binary

	Quadratic Forms
CO7	Understand Gauss Lemma, Jacobi symbol and its properties and Pell's Equation, Diophantine Equation
CO8	Understand Algebraic Number Fields and the Ring of Integers, Units and Primes.
CO9	Understand Dirichlet series with simple properties. Dirichlet series as analytic function and its derivative. Eulers products.
CO10	Understand existence of primitive roots. The group of quadratic residues. Quadratic residues for prime power moduli and arbitrary.

Syllabus:

ALGEBRAIC NUBER THEORY

Gaussian integers and its properties. Primes and fundamental theorem in the ring of Gaussian integers. Integers and fundamental theorem in Q (w) where w3 = 1, algebraic fields. Primitive polynomials. The general quadratic field Q(√m), Units of Q (√2). Fields in which fundamental theorem is false. Real and complex Euclidean fields. Fermat" theorem in the ring of Gaussian integers. Primes of Q(2) and Q(5). Luca" test for the prmality of the Mersenne number.

Arithmetical function φ(n), μ(n), d(n) and σ(n) Mobius inversion formulae. Perfect numbers. Order and average order of d(n), φ(n). The functions ϑ(x), ψ(x) and Δ(x). Betrand postulate. Sum p–1 and product 1+p–1. Merten's theorem Selberg's theorem. Prime number Theorem.

Integral elements in commutative ring extensions. Dedekind rings, their ideal theory and ideal classgroup. Fundamental theorem of Dedekind rings. Quadratic number fields. Cyclotomic fields and cyclotomic integers. Regular and irregular primes. Kummer's lemma. Kummer's proof of Fermat's great theorem for regular prime exponents. Norm and trace of an algebraic number. Ramification index and residue class degree of a prime ideal with respect to an algebraic field extension. Discriminant of an algebraic number field. Lattices in R^n and their quotient torus. Minkowski's theorem.

ANALYTICAL NUBER THEORY

Primes in certain arithmetical progressions. Fermat numbers and Mersenne numbers. Farey series and some results concerning Fary series. Approximtion of irrational numbers by rations. Hurwitz's theorem irrationality of e and n. The series of Fibonocci and Lucas. System of linear congruences Chinese Remainder Theorem. Congruence to prime power modulus.

Quadratic residues and non-residues. Legender's Symbol. Gauss Lemma and its applications. Quadratic Law of Reciprocity jacobi's Symbol. The arithmetic in Zp . The group Un . Primitive roots. The group Up n (p-odd) and U2 n . The existence of primitive roots. The group of quadratic residues. Quadratic residues for prime power moduli and arbitrary.

Riemann Zeta Function ξ(s) and its convergence. Application to prime numbers. ξ (s) as Euler's product. Evaluation of ξ(2) and ξ(2k). Dirichlet series with simple properties. Dirichlet series as analytic function and its derivative. Eulers products. Introduction to modular forms.

Resources
Name of Text and Reference Books:

1. Burton, David M. Elementary Number Theory. Allyn and Bacon, 1976.
2. Ireland, Kenneth F., and Michael I. Rosen, A classical Introduction to Modern Number Theory, Springer 1990.
3. G.A. Jones & J.M. Jones, Elementary Number Theory, Springer, UTM, 2007.
4. Neal Koblitz, A Course in Number Theory and Cryptography, Springer, Verlag - New york Inc., May 2001.
5. I. Niven, H. S. Zuckerman, H. L. Montgomery, \An Introduction to the Theory of Numbers", Wiley-India Edition, 2008.
6. T. M. Apostol, \Introduction to Analytic Number Theory", Springer International
7. Student Edition, 2000.
8. Cassels, J.W.S., Frolich, A., Algebraic Number Theory, Cambridge

CO-PO&PSO Correlation

Course Name : Number Theory										
	Program Outcomes						PSOs			
Course	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**
CO1:		2					3			
CO2:	1							2		
CO3:			2				2			
CO4:		2		1						1
CO5:	1		3					1		
CO6:		2					1			
CO7:	1				1			1		
CO8:		2							2	
CO9:			1				3			
CO10:		1				1		2		

Note: 1: Low 2: Moderate 3: High

Programme:	**PhD(Course Work)**	**Semester :**	
Name of the Course:	**Cryptography**	**Course Code:**	**PMA 108**
Credits :	**5**	**No of Hours :**	**50**
Max Marks:	**100**		

Course Description:

This Course focuses towards the introduction of network security using various cryptographic algorithms. Underlying network security applications. It also focuses on the practical applications that have been implemented and are in use to provide email and web security.

COURSE OUTCOMES:

On successful completion of this course, students will be able to:

CO Number	Course Outcome
CO1	Describe basic definitions and the Concepts of Security: The need for security
CO2	Understand Cryptographic Techniques.
CO3	Understand Computer-based Symmetric Key Cryptographic Algorithms
CO4	Understand Asymmetric Key Cryptography, An overview of Asymmetric Key Cryptography.
CO5	Understand Digital Signatures, Knapsack Algorithm, Some other algorithms.
CO6	Understand Digital Certificates, Private Key Management
CO7	UnderstandInternet Security Protocols
CO8	UnderstandE-mail Security, Wireless Application Protocol (WAP) Security, Security in GSM..

CO9	Understand Fixing Faults, Unexpected Behavior, Types of Flaws; Non-malicious Program Errors – Buffer Overflows, Incomplete Mediation.
CO10	Understand Trapdoors, Causes of Trapdoors; Methods of Control – Developmental Controls, Operating System Controls on use of Programs, Administrative Controls.

Syllabus:

Unit I

Computer-based Symmetric Key Cryptographic Algorithms: Algorithm Types and Modes, An overview of Symmetric Key Cryptography, DES, International Data Encryption Algorithm (IDEA), RC5, Blowfish, AES, Differential and Linear Cryptanalysis.

Unit II

Computer-based Asymmetric Key Cryptography: Brief History of Asymmetric Key Cryptography, An overview of Asymmetric Key Cryptography, The RSA Algorithm, Symmetric and Asymmetric Key Cryptography Together, Digital Signatures, Knapsack Algorithm, Some other Algorithms.

Unit III

Public Key Infrastructure: Digital Certificates, Private Key Management, The PKIX Model, Public Key Cryptography Standards, XML, PKI and Security. Internet Security Protocols: Basic Concepts, Secure Socket Layer, SHTTP.

Unit IV

Protection of Computing Resources: Secure Programs – Fixing Faults, Unexpected Behavior, Types of Flaws; Non-malicious Program Errors – Buffer Overflows, Incomplete Mediation; Viruses and Other Malicious Code – Kinds of Malicious Code, Virus Attack, Appended Virus; Targeted Malicious Code – Trapdoors, Causes of Trapdoors; Methods of Control – Developmental Controls, Operating System Controls on use of Programs, Administrative Controls.

Reference Books:

1. Cryptography And Network Security Principles And Practice Fourth Edition, William Stallings, Pearson Education.
2. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall PTR.
3. Network Security Essentials: Applications and Standards, by William Stallings. Prentice Hall.
4. Cryptography: Theory and Practice by Douglas R. Stinson, CRC press.

O P JINDAL UNIVERSITY

O P Jindal Knowledge Park, Punjipathra, Raigarh-496109
School of Science, Department of Mathematics

OPJU
UNIVERSITY OF STEEL TECHNOLOGY AND MANAGEMENT

CO-PO&PSO Correlation

Course Name : Cryptography										
	Program Outcomes						PSOs			
Course	**1**	**2**	**3**	**4**	**5**	**6**	**1**	**2**	**3**	**4**
CO1:		2					3			
CO2:	1							2		
CO3:			2				2			
CO4:		2		1						1
CO5:	1		3					1		
CO6:		2					1			
CO7:	1				1			1		
CO8:		2							2	
CO9:			1				3			
CO10:		1				1		2		

Note: 1: Low 2: Moderate 3: High