APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

(A State Government University)

B. Tech, 2024

Honours Degree in

Computer Science and Engineering

CURRICULUM

- **Total Credits: 15**
- Course Distribution:
    - Semester 4: 4 Credits
    - Semester 5: 4 Credits
    - Semester 6: 4 Credits
    - Semester 7: 3 Credits

Honours in Computer Science and Engineering

Sl. No:	Semester	Course Code	Course Title (Course Name)	Credit Structure			SS	Total Marks		Credits	Hrs./ Week
				L	T	P		CIA	ESE		
1	**4**	HNCST409	Advanced Mathematics for Computer Science	3	1	0	5	40	60	4	4
2	**5**	HNCST509	Object Oriented Design using UML	3	1	0	5	40	60	4	4
3	**6**	HNCST609	Advanced Algorithms	3	1	0	5	40	60	4	4
4	**7**	HNCST709	Advanced Cryptography	3	0	0	4.5	40	60	3	3
Total							**20**			**15**	**15**

XX: Branch/Department Code

SYLLABUS

SEMESTER 4

SEMESTER 4

Advanced Mathematics for Computer Science

Course Code	HNCST409	**CIE Marks**	40
Teaching Hours/Week (L:T:P)	3:1:0	ESE Marks	60
Credits	4	Exam Hours	2 Hrs. 30 Min.
Prerequisites (if any)	GAMAT201, PCCST201, GAMAT301	Course Type	Theory

Course Objectives:

1. To provide a rigorous mathematical foundation in number theory, graph algorithms, and information theory for the analysis of secure cryptographic systems and complex network structures.
2. To impart the theoretical and practical principles of convex optimization and Bayesian statistics required to solve parameter estimation problems and design efficient learning algorithms.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	Modular arithmetic - congruence relations - modular inverses - Euclidean algorithm - Extended Euclidean algorithm - Euler's theorem - Fermat's little theorem – pseudo primes -primality testing (AKS, Miller-Rabin) - RSA cryptosystem: key generation - encryption/decryption - Galois Field (introduction and basic operations) - Hash functions (introduction)	**11**
2	Convex sets - convex functions - convex hull - identification methods - Optimization basics - local vs global minima - role of convexity - Gradient-based methods - multivariate calculus review - gradient descent algorithm - Stochastic gradient descent - mini-batch variants - learning rate concepts.	**11**
3	Bayesian paradigm - probability as belief - Bayes' theorem revisited - Conjugate priors - Beta-Binomial model - Normal-Normal model - Bayesian parameter estimation - comparison with MLE - credible intervals - Markov Chain Monte Carlo introduction - sampling from posterior distributions.	**11**
4	Graph theory review - shortest path algorithms - Dijkstra's algorithm and its improvement - Network flow - max-flow min-cut theorem - PageRank algorithm - Information theory - entropy - cross-entropy - KL divergence	**11**

Course Assessment Method
(CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

	Course Outcome	Bloom's Knowledge Level (KL)
CO1	Solve modular arithmetic problems and congruence relations using the Extended Euclidean algorithm to execute RSA key generation, encryption, and decryption.	**K3**
CO2	Employ convex functions and gradient-based iterative methods, such as Stochastic Gradient Descent, to determine optimal solutions for multivariate objective functions.	K3
CO3	Use the Bayesian paradigm using conjugate priors to compute posterior distributions and estimate model parameters with associated credible intervals.	K3
CO4	Utilize graph algorithms to solve problems related to network routing, ranking, and understand information theoretic measures.	K3

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	3	3		2	2						3
CO2	3	3		2	2						3
CO3	3	3		2	2						3
CO4	3	3		2	2						3

Text Books

Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1	A course in number theory and cryptography	Koblitz, Neal.	Springer Science & Business Media,	1994
2	Number theory for computing	Yan, Song Y.	Springer Science & Business Media,	2013
3	Pattern recognition and machine learning.	Christopher M. Bishop	Springer	2009
4	Convex optimization for machine learning	Changho Suh	now Publishers Inc	2022

Reference Books

Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1	Machine Learning: A Probabilistic Perspective	Murphy, K. P.	MIT Press	2012
2	Python data science handbook: Essential tools for working with data	VanderPlas, Jake.	O'Reilly Media, Inc.	2016

Video Links (NPTEL, SWAYAM…)

Module No.	Link ID
1	https://onlinecourses.nptel.ac.in/noc22_cs90/preview
2	https://nptel.ac.in/courses/106101466
3	https://onlinecourses.swayam2.ac.in/imb21_mg03/preview
4	https://nptel.ac.in/courses/106106131 https://nptel.ac.in/courses/106105031

MODEL QUESTION PAPER

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
FOURTH SEMESTER B. TECH HONOURS DEGREE EXAMINATION, MONTH AND YEAR

Course Code:

Course Name: Computational Mathematics for Computer Science and Applications

Max. Marks: 60		Duration: 2 hours 30 minutes

PART A

		Answer all questions. Each question carries 3 marks	CO	Marks
1		Show that congruence is an equivalence relation.	1	(3)
2		Find the last two digits of 99^{1247}.	1	(3)
3		Define convex sets and convex functions with examples.	2	(3)
4		Explain the working principle of gradient descent algorithm.	2	(3)
5		What are conjugate priors and why are they useful in Bayesian inference?	3	(3)
6		What are the main features of Beta-Binomial model.	3	(3)
7		Describe the PageRank algorithm and its applications.	4	(3)
8		Explain the concept of Markov Decision Processes in reinforcement learning.	4	(3)

PART B

Answer any one full question from each module. Each question carries 9 marks

Module 1

9	a)	Find the GCD of 1071 and 462 using extended Euclidean algorithm and express this GCD as a linear combination of 1071 and 462	1	5
	b)	Compute $\phi(77)$ and explain its significance in RSA cryptography	1	4
10	a)	Solve the system of congruence equations: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$	1	5
	b)	Explain Fermat's Little Theorem and demonstrate its application in primality testing.	1	4

Module 2

11	a)	Explain one iteration of gradient descent for the function $f(x) = x^2$ starting from $x = 4$ with learning rate $\eta = 0.1$.	2	5
	b)	Compare the convergence behaviour of Batch Gradient Descent and Stochastic Gradient Descent.	2	4
12	a)	Derive the gradient update rule for linear regression using mean	2	5

		squared error loss		
	b)	Check whether the function $f(x,y)=x^2+y^2$ is convex and justify your answer	2	4
Module 3				
13	a)	Explain the concept of Markov Chain Monte Carlo and its role in Bayesian computation.	3	5
	b)	Implement Bayesian inference for a coin toss experiment with Beta prior and Binomial likelihood.	3	4
14	a)	Derive the conjugate prior for Poisson distribution and show the posterior distribution.	3	5
	b)	Explain how MCMC sampling helps in approximating complex posterior distributions.	3	4
Module 4				
15	a)	Explain PageRank algorithm.	4	5
	b)	Compute entropy for a given probability distribution and explain its significance.	4	4
16	a)	Explain the significance of dijkstra algorithm with a suitable example	4	5
	b)	Differentiate KL divergence and cross entropy	4	4
*****				

SEMESTER 5

SEMESTER 5

Object Oriented Design Using UML

Course Code	HNCST509	**CIE Marks**	40
Teaching Hours/Week (L:T:P)	3:1:0	ESE Marks	60
Credits	4	Exam Hours	2 Hrs. 30 Min.
Prerequisites (if any)		Course Type	Theory

Course Objectives:

1. To master the fundamental principles of object-oriented methodology—including abstraction, encapsulation, and inheritance—and apply analysis techniques to model the static and dynamic behavior of software systems.
2. To implement rigorous system and object design strategies and utilize the Unified Modeling Language (UML) along with standard design patterns to construct robust, scalable software architectures.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	Introduction: Object Oriented Development - Modeling Concepts– Object Oriented Methodology. Object Oriented Themes - Abstraction - Encapsulation - Combining Data and Behavior - Sharing - Emphasis on Object Structure. Object Oriented Models. Object modeling: Objects and Classes, Links and Associations, Advanced links and Association Concepts, Generalization and Inheritance, Grouping Constructs, A Sample Object Model.	**11**
2	Dynamic modeling: Events and States, Operations, Nested state diagrams, Concurrency, Advanced Dynamic Modeling Concepts, A sample Dynamic Model, Relationship of Object and Dynamic models. Functional modeling: Functional models, Data Flow Diagrams, Specifying Operations, Constraints, A sample Functional Model. Analysis: Object Modeling - Identifying Object Classes - Preparing a Data Dictionary - Identifying Associations. Dynamic Modeling - Preparing a Scenario - Interface Format - Identifying Event - Building a State Diagram. Functional Modeling - Identifying input and Output Values - Building Data Flow Diagram-Describing Functions.	**11**

3	System Design: Breaking System into Subsystems, Identifying Concurrency, Allocating Subsystems to Processors and Tasks, Managing Data Stores, Handling of Global Resources, Common Architectural Framework. Object Design: Overview of Object design, Combining the three models, Designing algorithms, Design optimization, Implementation of control, Adjustment of inheritance, Design of association, Object representation, Physical packaging. Documenting design decisions - Comparison of methodologies.	**11**
4	Unified Modeling Language (UML)-UML introduction & benefits-Different types of UML diagrams- Behavioral. Diagrams-Activity Diagram - Use Case Diagram - State Machine Diagram - Sequence Diagram , structural diagrams.- Class Diagram-Object Diagram-Component Diagram-Composite Structure Diagram-Deployment Diagram-Package Diagram. UML tools and their needs. Design Patterns-Creational - Structural – Behavioral.	**11**

Course Assessment Method
(CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Develop object models that represent the static structure of a real-world system by utilizing concepts such as classes, associations, generalization, and inheritance.	Apply
CO2	Develop dynamic and functional models using state transition diagrams and data flow diagrams to capture system events, concurrency, and operational requirements.	Apply
CO3	Translate analysis models into detailed system and object designs by defining subsystems, optimizing algorithms, and managing data storage strategies.	Apply
CO4	Solve real time problems using various Modeling concepts for managing projects in multidisciplinary environments	Apply

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	3	3	3								3
CO2	3	3	3	3							3
CO3	3	3	3	3							3
CO4	3	3	3	3							3

Text Books

Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1	Object Oriented Modeling and Design	James Rumbaugh	Prentice Hall India	1/e
2	Object Oriented Analysis and Design with Applications	Grady Booch	Pearson Education Asia References	3/e
3	UML Distilled: A Brief Guide to the Standard Object Modeling Language	Martin Fowler	Addison-Wesley Professional	3/e

Reference Books

Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1	Object Oriented Software Engineering	Ivan Jacobson	Pearson Education Asia.	3/e
2	Object Oriented Software	Berno Bruegge, Allen H.	Pearson Education	3/e

	Engineering	Dutoit	Asia.	
3	Object Oriented Analysis and Design using UML	H. Srimathi, H. Sriram, A. Krishnamoorthy	Scitech Publications.	1/e
4	UML and C++ practical guide to Object Oriented development	Richard C.Lee& William	Prentice Hall India	2/e.

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	**https://nptel.ac.in/courses/106105224**

MODEL QUESTION PAPER

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIFTH SEMESTER B. TECH HONOURS DEGREE EXAMINATION, MONTH AND YEAR

Course Code:

Course Name:

Max. Marks: 60		Duration: 2 hours 30 minutes

		PART A		
		Answer all questions. Each question carries 3 marks	CO	Marks
1		List and define the three models in object oriented methodology.	1	(3)
2		Differentiate aggregation and composition in object oriented methodology with example.	1	(3)
3		Define the terms event and state in the context of dynamic modelling.	2	(3)
4		Describe the concept of interface format in dynamic modeling.	2	(3)
5		What are the adjustments that can be done to increase the chance of inheritance?	3	(3)
6		What are the factors to be considered for the design of the algorithm by a designer?	3	(3)
7		Explain Unified Modeling Language (UML).	4	(3)
8		Mention the purpose of use case diagram.	4	(3)
		PART B		
		Answer any one full question from each module. Each question carries 9 marks		
		Module 1		
9	a)	What is object oriented methodology? Explain the stages involved in the object oriented methodology.	1	14
10	a)	Explain the different Object-Oriented Themes.	1	14
		Module 2		
11	a)	Describe process, data flow and datastore used in data flow diagrams with example.	2	14

12	a)	Explain the concept of dynamic modeling and the steps performed for constructing a dynamic model.	2	14
Module 3				
13	a)	How the design optimization is performed?	3	7
	b)	Explain the concept of documenting design decisions in object design and its importance for maintaining consistency, understanding, and future modifications.	3	7
14	a)	Explain physical packaging in object design.	3	7
	b)	What are the three basic approaches to implementing the dynamic model?	3	7
Module 4				
15	a)	Explain the Unified Modeling Language (UML) and its role in object-oriented analysis and design.	4	14
16	a)	Explain the different types of design patterns.	4	14
*****				

SEMESTER 6

SEMESTER 6

Advanced Algorithms

Course Code	HNCST609	CIE Marks	40
Teaching Hours/Week (L:T:P)	3:1:0	ESE Marks	60
Credits	4	Exam Hours	2 Hrs. 30 Min.
Prerequisites (if any)	PCCST502	Course Type	Theory

Course Objectives:

1. To introduce advanced algorithmic techniques and theoretical tools for analyzing complex problems.
2. To enable students to design and evaluate efficient solutions using dynamic, greedy, randomized, and approximation strategies.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	Advanced recurrence forms, Akra-Bazzi Theorem, Dynamic Programming - Longest Common Subsequences, Bellman Ford algorithm, Backtracking - Subset Sum, Hamiltonian Path (concept only), Branch and Bound - Knapsack problem, Greedy Method - Huffman codes, Matroids. Space-Bounded Computations - Basic concepts of L & NL, Space hierarchy (introductory), Savitch's Theorem (concept only).	11
2	Sorting Networks - Comparison Networks, Zero-One Principle, Bitonic Sorting Network - structure & analysis, Merging Networks, Batcher's Odd-Even Mergesort Network, Complexity of Sorting Networks (depth & size). String Matching Algorithms - The Naïve Pattern Matching Algorithm, Rabin–Karp Algorithm - analysis using hashing, Finite Automata-based String Matching, Knuth -Morris-Pratt (KMP) Algorithm - prefix function, analysis.	11
3	Randomization - Basic Probability - indicator variables, inequalities & Bounds - Markov's Inequality, Chebyshev's Inequality, Chernoff Bound (applications only) - Universal Hashing - Expectations, Markov Chains and Random Walks, 2-SAT random walk, random walks on graphs (concept only), Applications of Randomized Algorithms.	11

4	Approximation Algorithms - Approximation Algorithms for NP -Hard Problems - Approximation Algorithms for the Vector cover problem, Traveling Salesman Problem - Knapsack Problem, Algorithms for Solving Nonlinear Equations - Bisection Method - Method of False Position - Newton's Method.	11

Course Assessment Method
(CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Explain advanced algorithmic concepts such as recurrence solving, sorting networks, randomized bounds and space-bounded computations.	K2
CO2	Summarize key algorithmic strategies including dynamic programming, greedy methods, backtracking and approximation techniques.	K2
CO3	Apply dynamic programming, greedy and randomized methods	K3

	to solve problems such as LCS, Bellman-Ford, KMP and hashing-related tasks.	
CO4	Apply approximation algorithms and numerical methods to obtain solutions for NP-hard problems and nonlinear equations.	K3

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**
CO1	3	3	3	2							2
CO2	3	3	3	2							2
CO3	3	3	3	2	2						2
CO4	3	3	3	2							2

Text Books

Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Introduction to Algorithms	Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein	MIT Press	4/e, 2022
2	Randomized Algorithms	Rajeev Motwani and Prabhakar Raghavan	Cambridge University Pres	1/e, 2004

Reference Books

Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Algorithms	Robert Sedgewick and Kevin Wayne	Addison-Wesley	4E, 2011
2	Algorithm Design	Jon Kleinberg & Éva Tardos	Addison–Wesley	1E, 2006
3	Introduction to the Theory of Computation	Michael Sipser	Cengage Learning	3E, 2012
4	Approximation Algorithms	Vijay V. Vazirani	Springer-Verlag Berlin Heidelberg	1E, 2001

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
1	https://onlinecourses.nptel.ac.in/noc20_cs39
2	https://onlinecourses.nptel.ac.in/noc23_cs01
3	https://www.digimat.in/nptel/courses/video/106105225
4	https://onlinecourses.nptel.ac.in/noc24_cs97

MODEL QUESTION PAPER

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SIXTH SEMESTER B. TECH HONOURS DEGREE EXAMINATION, MONTH AND YEAR

Course Code: HNCST609

Course Name: Advanced Algorithms

Max. Marks: 60		Duration: 2 hours 30 minutes

PART A

		Answer all questions. Each question carries 3 marks	CO	Mark
1		Differentiate between L and NL with suitable examples.	1	(3)
2		Explain how Bellman–Ford algorithm applies dynamic programming to handle negative edge weights.	3	(3)
3		State the Zero-One Principle and explain its significance in sorting networks.	1	(3)
4		Construct the prefix function (π table) for the pattern **“ababaca”** using the KMP algorithm.	3	(3)
5		State Markov’s Inequality and Chebyshev’s Inequality with their conditions of applicability.	1	(3)
6		Given a hash family H, show how Universal Hashing reduces collision probability in randomized algorithms.	3	(3)
7		Define approximation ratio. Illustrate with an example for a simple NP-hard problem.	2	(3)
8		Apply the Bisection Method to approximate a root of the equation $f(x)=x^3-4x+1$ in the interval [0, 2] for one iteration.	4	(3)

PART B				
Answer any one full question from each module. Each question carries 9 marks				
Module 1				
9	a)	Explain the Akra–Bazzi Theorem. Illustrate with the recurrence: T(n)=T(n/2)+T(n/3)+n	1	(4)
	b)	Using backtracking, solve the Subset Sum problem for: S = {3, 5, 7, 10}, Target = 15. Show the search tree up to the first solution.	3	(5)
10	a)	Describe the structure of matroids. Explain how the greedy method is justified using matroid properties.	1	(4)
	b)	Apply Branch and Bound to solve the 0/1 Knapsack problem for the following items: Weights = {2, 3, 4, 5}, Profits = {3, 4, 5, 8}, Capacity=5. Draw the state-space tree and bound calculations.	3	(5)
Module 2				
11	a)	Explain the structure and working of a Bitonic Sorting Network with neat diagram.	1	(4)
	b)	Construct the DFA table for the Finite Automata-based String Matching algorithm for the pattern **“aba”** over alphabet {a, b}.	3	(5)
12	a)	Explain Batcher’s Odd-Even Mergesort Network. Discuss its depth and size.	1	(4)
	b)	Given the text **T = “3245532453”** and pattern **P = “245”**, perform Rabin Karp pattern matching with modulo 11. Show the rolling hash calculations.	3	(5)
Module 3				
13	a)	Define indicator variables and derive expected value of the number of heads in ‘n’ biased coin tosses.	1	(4)
	b)	Explain the randomized algorithm for 2-SAT using random walks. Apply one iteration to a small example.	3	(5)
14	a)	Explain Markov Chains and stationary distributions with a simple example.	1	(4)
	b)	Apply Chernoff Bound to estimate the probability that the number of heads in 100 fair coin tosses deviates from the mean by more than 20.	3	(5)
Module 4				

15	a)	Explain the approximation algorithm for the Vertex Cover problem. Discuss approximation ratio.	2	(4)
	b)	Using Newton’s Method, compute one iteration to find the root of $f(x) = x^2 - 5x+6$, starting at $x_0=0$.	4	(5)
16	a)	Describe the approximation algorithm for metric TSP using Minimum Spanning Tree.	2	(4)
	b)	Solve one iteration of the Method of False Position for $f(x)=x^3-x-1$, over the interval [1, 2].	4	(5)
*****				

SEMESTER 7

SEMESTER 7

Advanced Cryptography

Course Code	**HNCS709**	**CIE Marks**	40
Teaching Hours/Week (L:T:P)	3:0:0	ESE Marks	60
Credits	3	Exam Hours	2 Hrs. 30 Min.
Prerequisites (if any)		Course Type	Theory

Course Objectives:

1. To equip the learner in the theoretical foundations of quantum mechanics and quantum algorithms, such as Shor’s and Grover’s, in order to evaluate their destabilizing impact on classical public-key cryptography and understand the principles of quantum key distribution.
2. To investigate the mathematical hard problems and design principles underlying post-quantum cryptographic families—specifically hash-based, code-based, lattice-based, and multivariate systems—to develop secure alternatives resilient against quantum adversaries.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	Quantum Computing-Introduction, Quantum mechanics Shor's Factoring Algorithm-Factoring, Reduction from factoring to period-finding, Shor's period-finding algorithm, Continued fractions Grover's Search Algorithm, Quantum Cryptography-Saving cryptography from Shor, Quantum key distribution, Reduced density matrices and the Schmidt decomposition, The impossibility of perfect bit commitment, More quantum cryptography (Quantum Computing: Lecture Notes- Ronald de Wolf)	9
2	Introduction to post-quantum cryptography- Is cryptography dead?, A taste of post-quantum cryptography, Challenges in post-quantum cryptography, Comparison to quantum cryptography Classical Cryptography and Quantum computing, The computational model, The quantum Fourier transform, The hidden subgroup problem	9
3	Hash-based Digital Signature Schemes-Hash based one-time signature schemes, Merkle’s tree authentication scheme, One-time key-pair generation using an PRNG, Authentication path computation, Tree chaining, Distributed signature generation, Security of the Merkle Signature Scheme Code-based cryptography-Introduction, Cryptosystems, The security	9

	of computing syndromes as one-way function, Codes and structures	
4	Lattice-based Cryptography-Introduction, Preliminaries, Finding Short Vectors in Random *q*-ary Lattices, Hash Functions, Public Key Encryption Schemes, Digital Signature Schemes Multivariate Public Key Cryptography-Introduction, The Basics of Multivariate PKCs, Examples of Multivariate PKCs, Basic Constructions and Variations, Standard Attacks (module 2-4 -Post-Quantum Cryptography by Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen)	**9**

Course Assessment Method
(CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	Develop problem-solving and analytical skills in quantum computation	**K3**
CO2	Describe the foundations and goals of post-quantum cryptography	**K2**
CO3	Apply authentication mechanisms in hash-based systems and understand the foundations of code-based cryptography	**K3**
CO4	Apply lattice-based cryptographic constructions and Multivariate Public Key Cryptography for data security	**K3**

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	3	2	2								2
CO2	3										2
CO3	3	2	2								2
CO4	3	2	2								2

Text Books

Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1	Post-Quantum Cryptography	Daniel J. Bernstein · Johannes Buchmann Erik Dahmen	Springer	1/e,2009
2	Quantum Computing	Ronald de Wolf	QuSoft, CWI and University of Amsterdam	I/e, 2023

Reference Books

Sl. No	Title of the Book	Name of the Author/s	Name of the Publisher	Edition and Year
1				
2				
3				

Video Links (NPTEL, SWAYAM…)

Module No.	Link ID
1	
2	
3	
4	

MODEL QUESTION PAPER

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEVENTH SEMESTER B. TECH HONOURS DEGREE EXAMINATION, MONTH AND YEAR

Course Code:

Course Name:				
Max. Marks: 60			Duration: 2 hours 30 minutes	
		PART A		
		Answer all questions. Each question carries 3 marks	CO	Marks
1				(3)
2				(3)
3				(3)
4				(3)
5				(3)
6				(3)
7				(3)
8				(3)
PART B				
Answer any one full question from each module. Each question carries 9 marks				
Module 1				
9	a)			
	b)			
10	a)			
	b)			
Module 2				
11	a)			
	b)			
12	a)			
	b)			
Module 3				
13	a)			
	b)			
14	a)			
	b)			
Module 4				
15	a)			
	b)			
1	a)			

6	b)			
*****				