QUANTUM CRYPTOGRAPHY

Subject Code: CS34222CS	Subject Type: Elective
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 3-0-0

Pre-Requisites: Discrete Mathematics, Linear Algebra, Probability & Statistics, Theory of Computation, Computer Networks, Operating System, Data Structures & Algorithms, Programming Skills, and Computer Architecture.

Course Objective: To provide students with a strong foundation in quantum cryptography, quantum computing principles, and post-quantum security mechanisms. The course aims to introduce the mathematical and computational foundations of quantum information, quantum algorithms, quantum-resistant cryptographic systems, and secure communication protocols based on quantum mechanics. Additionally, the course enables students to understand the impact of quantum computing on modern cryptographic systems and design secure cryptographic solutions resilient against quantum attacks.

Course Outcomes: At the end of the course, the student will be able to

CO-1	Understand the fundamentals of quantum computing, quantum information theory, qubits, quantum gates, entanglement, and quantum computational models
CO-2	Analyze quantum algorithms including Deutsch-Jozsa, Bernstein-Vazirani, Grover's Algorithm, Quantum Fourier Transform, and Shor's Algorithm with respect to computational complexity and cryptographic implications
CO-3	Evaluate the impact of quantum computing on classical cryptographic systems including RSA, Diffie-Hellman, digital signatures, and public key infrastructures
CO-4	Understand post-quantum cryptographic approaches including lattice-based cryptography, code-based cryptography, quantum-resistant encryption schemes, and Learning with Errors (LWE)-based constructions
CO-5	Design and analyze secure quantum cryptographic protocols including Quantum Key Distribution (QKD), quantum encryption, quantum authentication mechanisms, and emerging quantum-secure communication systems

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	3	2	2	3	2
CO-2	3	3	3	2	3	2
CO-3	3	3	3	1	3	3
CO-4	3	3	3	2	3	2
CO-5	3	3	3	2	3	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1 Fundamentals of Quantum Computing and Quantum Information:

Introduction to Quantum Computing, Classical vs Quantum Computation, Mathematical Foundations of Quantum Mechanics, Qubits and Quantum States, Dirac Notation, Quantum Superposition, Quantum Entanglement, Quantum Gates and Quantum Circuits, Single and Multi-Qubit Systems, Quantum Parallelism, No-Cloning Theorem, Quantum Measurement Principles, Basics of Quantum Information Theory, Quantum Complexity Concepts, Introduction to Quantum Cryptography

Unit-2 Quantum Algorithms and Cryptographic Implications:

Quantum Algorithms: Deutsch Algorithm, Deutsch-Jozsa Algorithm, Simon's Algorithm, Bernstein-Vazirani Algorithm, Grover's Search Algorithm, Quantum Fourier Transform (QFT), Shor's Factoring Algorithm, Hidden Subgroup Problem, Computational Complexity of Quantum Algorithms, Impact of Quantum Computing on Classical Cryptography, Attacks on RSA, Diffie-Hellman and Discrete Logarithm Systems, Quantum Search Techniques, Quantum Oracle Models, Security Challenges in the Quantum Era

Unit-3 Post-Quantum Cryptography and Quantum-Resistant Security:

Introduction to Post-Quantum Cryptography, Quantum-Resistant Cryptographic Design, Lattice-Based Cryptography, Learning With Errors (LWE), Short Integer Solution (SIS) Problem, Code-Based Cryptography, Multivariate Cryptography, Isogeny-Based Cryptography, Quantum-Secure Public Key Encryption, Quantum-Secure Digital Signatures, Quantum Hardness Assumptions, Random Oracle Model in Quantum Settings, Homomorphic Encryption, Fully Homomorphic Encryption (FHE), Secure Key Exchange in Post-Quantum Environments

Unit-4 Quantum Cryptographic Protocols and Applications:

Quantum Key Distribution (QKD), BB84 Protocol, Quantum One-Time Pad, Quantum Encryption Schemes, Quantum Authentication, Quantum Public Key Encryption, Quantum Secure Communication Protocols, Quantum Randomness Generation, Quantum Money Concepts, Secure Multi-Party Quantum Communication, Quantum Cloud Security, Quantum Network Security, Blockchain and Quantum Security Challenges, AI and Quantum Security Applications, Emerging Trends in Quantum Cryptography, Practical Challenges in Quantum Computing and Security Implementations

Learning Resources:

Text Books:

1. Introduction to Modern Cryptography — Jonathan Katz and Yehuda Lindell, CRC Press.
2. Foundations of Cryptography — Oded Goldreich, CRC Press.
3. Quantum Computation and Quantum Information — Michael A. Nielsen and Isaac L. Chuang.
4. Modern Cryptography: Theory and Practice — Wenbo Mao, Pearson Education.
5. Post-Quantum Cryptography — Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, Springer.

Reference Books:

1. Understanding Quantum Information and Computation — Michael A. Nielsen.
2. Quantum Computing for Computer Scientists — Noson S. Yanofsky and Mirco A. Mannucci.
3. Introduction to Quantum Algorithms via Linear Algebra — Richard J. Lipton and Kenneth W. Regan.
4. Quantum Computer Science — N. David Mermin.
5. An Introduction to Quantum Computing — Phillip Kaye, Raymond Laflamme, and Michele Mosca.