

TABLE OF CONTENTS

Unit no.	Title	Page no.
1	Introduction to Post-Quantum Cryptography 1.1 Evolution of Cryptography: Classical to Quantum Era 1.2 Limitations of Classical Cryptographic Systems 1.3 Fundamentals of Quantum Computing and Cryptanalysis 1.4 Need for Post-Quantum Cryptography 1.5 Applications of Post-Quantum Security in Digital Systems	1
2	Mathematical Foundations of Post-Quantum Cryptography 2.1 Number Theory and Algebraic Structures 2.2 Lattice Theory and Hard Mathematical Problems 2.3 Error-Correcting Codes in Cryptography 2.4 Hash Functions and One-Way Transformations 2.5 Complexity Theory and Security Assumptions	15
3	Post-Quantum Cryptographic Algorithms 3.1 Lattice-Based Cryptography 3.2 Code-Based Cryptography 3.3 Multivariate Cryptography 3.4 Hash-Based Cryptography 3.5 Isogeny-Based Cryptograph	28
4	Quantum-Resistant Encryption and Digital Signatures 4.1 Post-Quantum Encryption Schemes 4.2 Key Exchange Mechanisms 4.3 Digital Signature Algorithms 4.4 Hybrid Cryptographic Approaches 4.5 Performance and Security Evaluation	45
5	Implementation of Post-Quantum Cryptography 5.1 Hardware and Software Implementations 5.2 Post-Quantum Cryptography in Embedded Systems 5.3 Cloud and Edge Computing Security 5.4 Blockchain and Distributed Systems Security 5.5 Implementation Challenges and Optimization Techniques	61
6	Standards and Real-World Deployment 6.1 NIST Post-Quantum Cryptography Standardization 6.2 Migration from Classical to Post-Quantum Systems 6.3 Security Protocol Integration	81

	6.4 Industrial and Government Applications 6.5 Case Studies of Post-Quantum Deployments	
7	Future Directions and Emerging Trends 7.1 Quantum-Safe Internet and Networks 7.2 Post-Quantum Cryptography for IoT Systems 7.3 AI and Post-Quantum Security 7.4 Open Research Challenges 7.5 Future of Quantum-Resistant Digital Systems	101
8	Security Analysis and Performance Evaluation of Post-Quantum Cryptography 8.1 Security Models and Threat Assessment in Post-Quantum Systems 8.2 Cryptanalytic Attacks on Post-Quantum Algorithms 8.3 Performance Metrics and Benchmarking Techniques 8.4 Scalability and Efficiency in Large-Scale Systems 8.5 Comparative Analysis of Post-Quantum Cryptographic Schemes	121
9	Post-Quantum Cryptography in Emerging Technologies 9.1 Post-Quantum Security for Internet of Things (IoT) 9.2 Post-Quantum Cryptography in Cloud Computing Environments 9.3 Quantum-Resistant Security for Blockchain and Distributed Ledgers 9.4 Post-Quantum Protection for 5G and Future Communication Networks 9.5 Applications of Post-Quantum Cryptography in Smart Cities and Cyber-Physical Systems	139
10	Post-Quantum Key Management and Secure Communication 10.1 Post-Quantum Key Distribution and Exchange Mechanisms 10.2 Authentication Protocols in Post-Quantum Systems 10.3 Secure Communication Protocols with Post-Quantum Algorithms 10.4 Integration of Post-Quantum Cryptography into Internet Security Protocols 10.5 Challenges and Future Research Directions in Quantum-Safe Communication	157