Modern Cryptography and AI/ML Security [3 0 0 3]		
Course Code: DSC XXX		
Prerequisites	DSC 314 or MAT 2012	
Proposed by	Dr. Laltu Sardar	
Learning Outcomes	● Explain the fundamental concepts, security definitions, and threat models of modern cryptography, including symmetric-key cryptography, public-key cryptography, hash functions, and MACs. ● Analyze the security challenges posed by quantum computing and the principles of post-quantum cryptography, including lattice-based assumptions and NIST-standardized schemes. ● Apply post-quantum cryptographic primitives and tools such as liboqs, OpenSSL, Kyber, and Dilithium for secure communication and hybrid cryptographic systems. ● Analyze security and privacy threats in AI/ML systems and compare privacy-preserving techniques used in secure AI/ML systems. ● Evaluate classical, post-quantum, and hybrid cryptographic solutions for secure system design with respect to security, performance, and deployment feasibility.	
Syllabus		**Hours**
	● Foundations of Cryptography: Security goals and threat models, Symmetric cryptography, Block ciphers and stream ciphers, Encryption and decryption, Hash functions, MACs, Authenticated encryption, PRG and PRP, One-way functions, Security definitions and reductions.	**4**
	● Public-Key Cryptography and Key Infrastructure: Integer factorization problem, Discrete logarithm problem, Elliptic curve discrete logarithm problem, RSA and ElGamal encryption, Elliptic curve Diffie-Hellman (ECDH), Digital signatures (RSA, ECDSA), Diffie-Hellman key exchange,	**3**
	● Public key infrastructure (PKI) and key management, Secret sharing, Identity-Based Encryption (IBE), Attribute-Based Encryption (ABE), Authenticated key exchange, TLS 1.3 overview.	**3**
	● Introduction to Post-Quantum Cryptography: Motivation for post-quantum cryptography, Quantum computing and cryptographic threats, Shor's algorithm, Grover's algorithm, NIST PQC standardization process,	**3**
	● Code-based cryptography, Hash-based signatures, Multivariate cryptography,	**3**

	• Isogeny-based cryptography, Hybrid classical and post-quantum cryptographic systems.	**3**
	• Lattice-Based Cryptography: Introduction to lattices, Properties of lattices, Shortest Vector Problem (SVP), Closest Vector Problem (CVP), Hardness assumptions (GapSVP, SIVP), Learning With Errors (LWE), Ring-LWE, Module-LWE,	**3**
	• Encryption and key encapsulation from lattices, CRYSTALS-Kyber, CRYSTALS-Dilithium, Security parameter selection and performance trade-offs.	**3**
	• Privacy-Preserving AI/ML Systems: Security and privacy in AI/ML systems, Differential privacy, Federated learning, Secure aggregation, Privacy-preserving inference, Secure model sharing and watermarking, Access control and authentication.	**4**
	• PQC Integration for AI/ML Systems: Post-quantum secure communication for AI/ML systems, Hybrid cryptographic systems,	**4**
	• Open Quantum Safe (OQS), liboqs, PQC integration with OpenSSL, Performance benchmarking and implementation considerations.	**3**
	• Advanced Topics in Modern Cryptography: Zero-knowledge proofs, Fully homomorphic encryption, Cryptographic agility and PQC migration strategies, Selected papers and recent advances in secure AI/ML systems.	**4**
Text & Reference Books	1. Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography”, CRC Press, 3rd edition, 2020. 2. Douglas R. Stinson, Maura Paterson, “Cryptography: Theory and Practice”, CRC Press, 4th edition, 2018. 3. Oded Goldreich, “Foundations of Cryptography: Basic Applications”, Cambridge University Press, 1st edition, 2004. 4. David Boneh, Victor Shoup, “A Graduate Course in Applied Cryptography”, Draft edition, 2023. 5. D. J. Bernstein, Johannes Buchmann, Erik Dahmen, “Post-Quantum Cryptography”, Springer, 1st edition, 2009. 6. J. Morris Chang, Di Zhuang, Dumindu Samaraweera, “Privacy-Preserving Machine Learning”, CRC Press, 1st edition, 2022.	