TE 582: Advanced Cryptography and Network Security

Duration: 3 weeks (27 hours/week)

Schedule: 3 hours/day × 3 days/week

Format: Lectures (theory) + Research Seminars + Guided Literature Reviews + Mini-Projects

Course Objectives

- Deep theoretical grounding in classical and modern cryptography.
- Research exposure to quantum and post-quantum cryptography.
- Ability to critically analyze protocols using an information-theoretic approach.
- Develop research questions leading to publishable work.
- Understand how cryptographic primitives integrate into network security models.

Weekly Outline

Week 1 – Foundations & Classical-to-Modern Cryptography

Day & Topic	**Content**
Day 1: Information-Theoretic and Complexity-Theoretic Security	Shannon's perfect secrecy model, one-time pad; Security definitions: IND-CPA, IND-CCA; Complexity assumptions; Limitations in quantum era; Research session on provable security problems.
Day 2: Modern Symmetric & Asymmetric Primitives	AES, ChaCha20, authenticated encryption; RSA, ECC, lattice intro; Secure key exchange; Literature review workshop.
Day 3: Network Security Models & Threats	OSI security architecture; Common attacks; PKI and certificate transparency; TLS 1.3 & QUIC; Mini-project kickoff on TLS vulnerabilities.

Week 2 – Quantum Cryptography & Post-Quantum Cryptography

Day & Topic	**Content**
Day 4: Quantum Computation Basics for Cryptographers	Qubits, superposition, entanglement; Quantum gates & algorithms; Impact on RSA/ECC; NIST PQC discussion.

Day 5: Quantum Key Distribution (QKD)	BB84, E91; Security proofs; Practical QKD; Simulation of BB84 in Python/QuTiP.
Day 6: Quantum-Resistant Cryptography	Lattice-based: NTRU, Kyber, Dilithium; Code-based: McEliece; Hash-based: XMSS, SPHINCS+; Multivariate polynomial cryptosystems; Research proposal brainstorming.

Week 3 – Research Applications & Emerging Topics

Day & Topic	**Content**
Day 7: Secure Multi-Party Computation (MPC) & Homomorphic Encryption	MPC protocols; Fully Homomorphic Encryption; Quantum-safe MPC; Research topic lab on FHE & lattice-based schemes.
Day 8: Blockchain & Distributed Ledger Cryptography	Consensus protocols; Cryptographic hash functions; PQ-secure blockchain proposals; Student research presentations.
Day 9: Future Directions & Research Methodology	Hybrid classical-quantum models; ZKPs in PQ context; Trends in protocol verification; Final project workshop.

Assessment & Deliverables

- Mini Research Proposal – 40%
- Practical Simulation/Implementation Report – 30%
- Class Participation & Literature Critique – 30%

Potential Research Topics

- Information-theoretic analysis of hybrid QKD–Post-Quantum key exchange protocols.
- Lattice-based secure routing in quantum-threatened networks.
- Post-quantum Zero-Knowledge Proofs for identity verification in IoT.
- Energy-efficient QKD protocols for 5G/6G networks.
- Post-quantum blockchain consensus mechanisms.
- Combining homomorphic encryption and quantum-resistant algorithms for secure cloud computing.