Course Title: **Post-Quantum Cryptography**

Credit Hrs: **3**

Prerequisites: Basic number theory

Defense Relevance: Critical for protecting military communications against quantum computer attacks

Course Objectives:

1. Understand vulnerabilities of current cryptographic systems
2. Master post-quantum cryptographic algorithms
3. Design quantum-resistant security protocols

Course Learning Outcomes: Students will be able to:

1. Analyze quantum attacks on classical cryptography
2. Implement lattice-based and code-based cryptographic schemes
3. Design hybrid classical-quantum security protocols
4. Evaluate post-quantum algorithm performance and security

Course Contents:

Week	Content
1-2	Quantum threats to classical cryptography
3-4	Lattice-based cryptography fundamentals
5-6	Learning with errors and ring-LWE
7-8	Code-based cryptographic systems
9-10	Multivariate public key cryptography
11-12	Hash-based digital signatures
13-14	Isogeny-based cryptography
15-16	Implementation and standardization

Textbooks/ References:

1. Bernstein, D.J. "Post-Quantum Cryptography" (2020)
2. Peikert, C. "A Decade of Lattice Cryptography" (2016)

Assessments:

1. Assignment: 10%
2. Quizzes: 10%
3. Midterm Exam: 30%
4. Final Exam: 40%