Course Number: COSC xxx

Course Title: Quantum Cryptography

Number of Credit Hours: 3

**Catalog Description**:

COSC xxx Quantum Cryptography – Three hours of lecture, 3 credits.

This course focuses on the field of quantum communications and quantum cryptography (often called Quantum Key Distribution). Topics will cover concepts necessary for implementing quantum communications systems including encryption, key distribution protocols, and post-quantum cryptographic techniques.

Prerequisite: COSC 323, COSC xxx Quantum Algorithms

**Course Objectives**

Upon completion of this course, students will be able to do the following:

• Describe quantum systems and protocols for quantum communications.

• Analyze techniques relevant to post-quantum cryptography

• Demonstrate skills by implementing and coding quantum algorithms.

**Course Content**

Unit 0: Review of classical cryptography

Unit 1: Quantum random number generation

Unit 2: Quantum key distribution protocols I

Unit 3: Quantum key distribution protocols II

Unit 4: Post-quantum cryptography overview

Unit 5: Post-quantum cryptography techniques I

Unit 6: Post-quantum cryptography techniques II

Unit 7: Quantum crypto project

**Course Schedule**

|  |  |  |  |
| --- | --- | --- | --- |
| **Week** | **Unit** | **Unit Name** | **Computer Lab/Project** |
|  |  |  |  |
| 1-3 | 0 | Review of classical cryptography | 1. Symmetric cryptography (AES) 2. Asymmetric cryptography (RSA) 3. Elliptic curves 4. Homomorphic crypto |
| 4 | 1 | Quantum random number generation | QRNG in depth |
| 5-6 | 2 | Quantum key distribution protocols I | 1. BB84 2. EK91 |
| 7-8 | 3 | Quantum key distribution protocols II | 1. COW 2. DPS |
| 9-10 | 4 | Post-quantum cryptography overview | 1. Shor’s algorithm 2. Database search of key spaces and AES 3. McEliece cryptosytem |
| 10-11 | 5 | Post-quantum cryptography techniques I | CRYSTALS-Kyber |
| 12-13 | 6 | Post-quantum cryptography techniques II | CRYSTALS-Dilithium |
| 14-15 | 7 | Quantum crypto project | Theoretical cryptanalysis of either RSA, Diffie-Hellman, elliptic curve, AES or lattice-based cryptography |
|  |  |  |  |

**Bibliography:**

• Quantum Computation and Quantum Information, M.A. Nielsen and I.L.Chuang, 10th Anniversary Edition. Cambridge. ISBN-13 ‏ : ‎ 978-1107002173, 2011.

• Fundamentals of Quantum Computing: Theory and Practice. Venkateswaran Kasirajan. Springer. ISBN-13: ‎ 978-3030636883, 2021.

* Understanding Cryptography: A textbook for students and practitioners, C. Paar and J. Pelzl, Springer, ISBN13 978-3642041006