**MATH 1800**

**Introduction to Quantum Information Theory with Applications to Cryptography**

**Syllabus**

# Overview

This is a one-semester introductory course in Quantum Information Theory. The main goal is to give the students an idea of the mathematics behind quantum algorithms and why in certain cases they are much more effective compared to their classical counterparts. After a brief introduction to Quantum Mechanics (mainly the principle of superposition), the basics of quantum computation and Discrete Fourier Transform, we will introduce one of the main quantum algorithms due to P. Shor. We will show how modifications of this algorithm can be applied to the two most important cryptosystems: RSA and ECC. We will also discuss possible effects that the emergence of a quantum computer would have on the standards of modern cryptography.

# Preliminary List of Topics

(1) A Brief Overview of Quantum Mechanics.

(2) Quantum Computation: Classical and Quantum Circuits.

(3) No-Cloning Theorem, and Quantum Teleportation.

(4) Discrete Fourier Transform and Fast Fourier Transform.

(5) Simon's Algorithm.

(6) Shor's Factoring Algorithm.

(7) Some Modifications (Applications) of Shor's Factoring Algorithm: DLP (discrete logarithm problem) and ECC (elliptic curve cryptography).

(8) The Hidden Subgroup Problem.

(9) Grover's Algorithm.

# Prerequisites

MATH 430 - Introduction to Abstract Algebraic Systems, MATH 0280 - Introduction to Matrices and Linear Algebra

# Texts

[NC00] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.