Syllabus for CYB 710
Introduction to Cryptography

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

Course Description

This course introduces the fundamentals of applied cryptography, including a survey of relevant mathematical concepts and elementary number theory, encryption and decryption, symmetric and asymmetric systems, block ciphers, hash functions, common attacks, digital signatures, key exchange, message authentication, public key cryptography, and implementation of cryptographic systems.

Prerequisite(s)

None

Program Outcomes

This course addresses the following competencies and program outcomes of the Master of Science in Cybersecurity:

- Program Outcome 1: Foundational – Students will describe key principles of cybersecurity.

Course Outcomes

- Upon completing this course, you will be able to do the following:
- Identify the elements of a cryptographic system.
- Describe the differences between symmetric and asymmetric algorithms.
- Describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
- Analyze the strengths and weaknesses of various cryptographic protocols and describe the issues that must be addressed in an implementation of a cryptographic system.

Course Requirements/Components

Self-Assessment Quizzes

The self-assessments consist of selected problems that you should know how to solve to succeed (or at least have less difficulty) when tackling some of the larger homework assignments and project elements in this course. You will have unlimited attempts to complete these quizzes.

Programming Assignments

Four short programming assignments are designed to give you practice implementing cryptographic concepts covered in the course.

Discussions

Discussions vary more in structure than the other assignments listed. All involve an initial post, with most requiring a response to at least one classmate's post. Discussions are designed to give you practice in both expressing your own ideas and collaborating with others in expanding and reasoning arguments and lines of inquiry.

Cryptography Assignments

These assignments (sometimes referred to as turn-in assignments in the course) have you delve into cryptography concepts in more detail and are meant to provide evidence that you understand the structure of a cryptographic protocol or mathematical procedure by writing down the details of the calculations involved in each step.

Course Project

A key part of this course involves completing a course project. This course project is done individually and will require you to demonstrate both a theoretical and practical understanding of the key concepts in this course. The project will be completed over the entire course and will involve five (5) deliverables, submitted as milestones distributed through the course. The final deliverable will put together the concepts from the other deliverables to implement a complete cryptographic system.

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	90% or greater
A-	87% - < 90%
B+	83% - < 87%
B	80% - < 83%
B-	77% - < 80%
C+	73% - < 77%
C	70% - < 73%
C-	65% - < 70%
F	0 - < 65%

Assignments	Percentage
Quizzes	5%
Programming Assignments	10%
Class Discussions	10%
Cryptography Assignments	35%
Course Project	40%
Total	100%