Master of Science in Cybersecurity

Syllabus for CYB775 Applied Cryptography

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

Course Description

An in-depth study of modern cryptography. Topics include public key and private key cryptography, types of attacks, cryptanalysis, perfect secrecy, hashing, digital signatures, virtual private networks, and quantum key cryptography. Topics from number theory and discrete probability necessary for understanding current cryptosystems and their security will be covered.

Prerequisite(s)

CYB 710: Introduction to Cryptography

Program Outcomes

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

- Program Outcome 4: Implement best practices in secure software development
- Program Outcome 5: Implement effective cryptographic systems and assess their vulnerabilities

Course Outcomes

Upon completing this course, you will be able to do the following:

- Identify and use public key and private key cryptosystems
- Identify different attacks and vulnerabilities for a cryptosystem
- Determine whether a cryptosystem is secure
- Create a Digital Signature Scheme to securely sign documents
- Implement hash functions

Course Requirements/Components

Describe what types of course components students will participate in such as discussions, quizzes, writing assignments, special projects, group work, etc. Each of these components can have a subheading.

Assignments

The primary assignments in this course consist of demonstrating your ability to execute the mathematical concepts through the completion of computation-based assignments and then implementing those concepts through by developing programs that execute various cryptographic functions (e.g., encrypt, decrypt, hash) for various cryptographic systems.

Discussions

In certain cases, the content requires research, analysis, and taking a stance, and providing justification (e.g., Quantum Cryptography). The discussions provide an opportunity for you to engage with your peers in this process, sharing your results, critically analyzing the work of others, and getting feedback on your work.

Final Project: Data Security & Privacy Review

The final project simulates a security review triggered by a change request in the hypothetical organization, you review this proposal and return an answer that points out the security flaws (if any) that are present. This assignment focuses only on the cryptographic issues with the systems. You may point out other flaws (networking, design, monitoring, etc.) if you wish, but they will not be part of your evaluation here. You will submit a report with three sections:

- **Executive Summary**: Write up an executive summary to management articulating the security of the system.
- **IT Summary:** Summarize the methods used for assessing vulnerabilities.
- **Technical Details:** Provide technical details supporting your findings.

Course Outline

Lesson 01: Introduction and Review of 710 Concepts
Lesson 02: Advanced Encryption Standard (AES)
Lesson 3: Discrete Log Problem & ElGamal
Lesson 4: Construction of the RSA Cryptosystem
Lesson 5: Factorization & RSA
Lesson 6: Hash Functions & Digital Signatures
Lesson 7: Elliptic Curves
Lesson 8: Discrete Probability and Statistics
Lesson 9: Virtual Private Networks and Cryptography
Lesson 10: Quantum Cryptography
Final Project

Grading

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

Grade	Percentage Range
A	94% - 100%
A-	90% - < 94%
B+	87% - < 90%
B	84% - < 87%
B-	80% - < 84%
C+	77% - < 80%
C	74% - < 77%
C-	70% - < 74%
F	0 - < 70%

Assignment	Percentage
Assignments	50%
Discussions	30%
Final Project	20%
Total Points	**100%**