Master of Science in Cybersecurity

Syllabus for CYB 775
Advanced 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 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:

- Perform attacks to identify and exploit vulnerabilities in public key cryptosystems
- Code various functions (methods) within the AES system to piece together a fully operational private key cryptosystem
- Determine whether a cryptosystem has perfect secrecy
- Identify various secure hash algorithms
- Code various functions (methods) within SHA-1 to build working knowledge of the SHA suite
- Identify how errors propagate through a cryptosystem
- Build a digital signature system to sign a document
- Describe various key distribution techniques for both public keys and private keys
- Identify risks associated that a key distribution technique may have
- Describe the basic principles of Identity-Based Cryptography
- Sign a digital message using an Identity-Based Digital Signature Scheme
- Perform algebraic operations (addition and multiplication) on elliptic curves
- Develop an Elgamal PKC on an elliptic curve
- 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 Legal and ethical considerations

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.

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%

Assignments	Percentage
Assignments	50%
Discussions	30%
Final Project	20%
Total	100%

AI Policy

AI use is not allowed in this course. Much of this course is designed to teach you the details that make modern cryptography work so that you can be prepared for attacks on systems you are working with. Using AI to solve the exercises will not help you understand the finer details to cryptosystems that make a system safe and secure.