# Syllabus for CYB 710 Introductory Cryptography

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

## Course Description

Fundamentals of applied cryptography, including encryption and decryption, symmetric and asymmetric systems, pseudorandom functions, block ciphers, hash functions, common attacks, digital signatures, key exchange, message authentication, and public-key cryptography. Implementation of cryptographic systems in an approved programming language. Survey of relevant mathematical concepts, including elementary number theory.

## Prerequisite(s)

None

## Program Outcomes

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

- Competency B: Design, develop, test, and evaluate secure software
  - Program Outcome 5: Implement effective cryptographic systems and assess their vulnerabilities
  - Program Outcome 4: Implement best practices in secure software development

## Course Outcomes

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

- Identify the elements and desired properties of a cryptographic system
- Understand the roles of, and differences between, symmetric and asymmetric systems
- Identify cryptographic tools and techniques appropriate for a given task
- Describe the strengths and weaknesses of various cryptographic algorithms and the issues involved in their effective implementation

## 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

For the final Project, you will be constructing an algorithm to design a secure message passing system. The programming assignment is designed to give you practice implementing some of the concepts needed for the final Project.

### 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.

As part of these assignments, you will be asked to explain your reasoning to problems that are more open-ended or which involve some choice on your part.

### Final Project: Secure Mail

A key part of this course involves completing a final project. This final 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 last five weeks of the course and will involve five (5) deliverables.

From a high-level perspective, you will design a secure message passing system, called **SecureMail**, for our users: senders ("Alice") and recipients ("Bob"). **SecureMail** should meet the following objectives:

i. **Confidentiality**: the messages Alice sends to Bob must be kept confidential and private from all third parties.
ii. **Non-repudiation**: Bob must be certain the message is coming from Alice, and vice versa.
iii. **Message integrity**: Bob must be certain the message from Alice has not been corrupted and is completely unaltered, and vice versa.
iv. **Computational efficiency**: Alice and Bob wish to use this system to send large messages to each other, so the run time of the overall process should be efficient.

Each of the five deliverables will be instrumental in meeting the above criteria.

## Grading

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

| Grade | Percentage Range |
|---|---|
| A | 90% - 100% |
| A- | 90% - < 94% |
| B+ | 87% - < 90% |
| B | 84% - < 87% |
| B- | 80% - < 84% |
| C+ | 76% - < 80% |
| C | 70% - < 76% |
| C- | 65% - < 70% |
| F | 0 - < 65% |

| Assignment | Percentages |
|---|---|
| Quizzes | 5% |
| Programming Assignments | 10% |
| Class Discussions | 10% |
| Cryptography Assignments | 35% |
| Final Project (100 pts)<br>• Deliverable 1 (10 pts)<br>• Deliverable 2 (30 pts)<br>• Deliverable 3 (20 pts)<br>• Deliverable 4 (20 pts)<br>• Deliverable 5 (20 pts) | 40%<br>• D1=4%<br>• D2=12%<br>• D3=8%<br>• D4=8%<br>• D5=8% |
| **Total** | **100%** |