UNIVERSITY OF THE DISTRICT OF COLUMBIA
SCHOOL OF ENGINEERING AND APPLIED SCIENCES

# Department of Computer Science and Information Technology
# Fall 2020

**Course Title: Cryptography - 15230 - CSCI 455 - 01**
**Instructor: Oladunni, Timothy**
**Office Location: Bldg. 42, Room 112 E**
**Class Location: Online**
**Instructor's Email: Timothy.oladunni@udc.edu**
**Class Hours: 2:00PM - 4:50PM F**
**Office Hours: 5:00PM- 7:00PM F**

## A. Course Description

This course examines the theory and application of cryptography. Topics include; Computer and Network Security Concepts, Classical Encryption Techniques, Block Ciphers and the Data Encryption Standard, Advanced Encryption Standard, Block Cipher Operation, Cryptographic Hash Functions, Message Authentication Codes, Digital Signatures, Key Management and Distribution etc.

## B. Course Objective

Students who complete this course should be able to perform the following tasks:

1. Explain symmetric/asymmetric encryption and decryption
2. Have an ability to do basic cryptanalysis
3. Have knowledge on mechanics of public-key cryptography
4. Have ability to use public-key encryption and illustrate the difference between symmetric and public- key cryptography.
5. Have ability to implement encryption and decryption algorithms

## C. Learning outcome

At the end of this course, students are expected to have understood:

- The principles and practice of cryptography

## D. Course Schedule (Tentative)

| Week | Topic | Lab/Test |
|---|---|---|
| **1.** | Computer and Network Security Concepts | |
| **2.** | Classical Encryption Techniques | Lab 1 |
| **3.** | Block Ciphers and the Data Encryption Standard | |
| **4.** | Advanced Encryption Standard | Test 1 |
| **5.** | Block Cipher Operation | **Lab 1 is due** Lab 2 |

| | | |
|---|---|---|
| **6.** | Random Bit Generation and Stream Ciphers | Test 2 |
| 7. | Midterm | |
| 8. | Project Proposal | |
| 9. | Public Key Cryptography and RSA | Test 3 |
| **10.** | Other Public-Key Cryptosystems | Lab 3<br>**Lab 2 is due** |
| **11.** | Cryptographic Hash Functions | |
| **12.** | Message Authentication Codes | Test 4 |
| **13.** | Project Presentation | **Lab 3 is due** |
| **14.** | Final | |

**E. Evaluation**

Final grade will be based on the following:

| | |
|---|---|
| Lab 1 | 5% |
| Lab 2 | 5% |
| Lab 3 | 5% |
| Test 1 | 10% |
| Test 2 | 10% |
| Test 3 | 10% |
| Test 4 | 10% |
| Mid Term | 15% |
| Attendance | 5% |
| Reflect on your learning experience by providing thoughtful feedback on course content and format | 5% |
| Project | 25% |
| Final | 15% |

**F. Textbook**

Cryptography and Network Security: Principles and Practice 7th Edition by William Stallings

**Laboratory**

Hands-On Cryptography with Python; Leverage the power of Python to encrypt and decrypt data by Samuel Bowne

**G. Format and Procedures**

This course will employ lectures, exercises, assignments, labs, and examinations. Students are strongly encouraged to participate extensively, ask questions, express ideas and opinions, and challenge traditional ideas and concepts. Instructional methodologies will emphasize critical thinking, problem solving, and reasoning over simple memorization.

**H. Assessment Procedures**

All students need to finish any given programming assignments in a timely manner. Assignments, tests, labs, and Final exam will take place to measure their ability of understanding cryptography.