Title: Cryptography - 15230 - CSCI 455 - 01
Instructor: Oladunni, Timothy
Office Location: Bldg. 42, Room 112 E
Class Location: C03
Instructor's Email: Timothy.oladunni@udc.edu
Class Hours: 12:30 pm - 1:50 pm TR
Office Hours: 2:00 pm- 4:00 pm TR

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. Learning outcome

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

- The principle and practice of cryptography

C. Course Schedule (Tentative)

Week	Topic	Python Topics	Lab/Test
1.	Computer and Network Security Concepts	Python Proficiency Test	
2.	Classical Encryption Techniques	Variables and Expressions	Lab 1
3.	Block Ciphers and the Data Encryption Standard	Types	
4.	Advanced Encryption Standard	Branching	
5.	Block Cipher Operation	Loops	**Lab 1 is due** Lab 2
6.	Random Bit Generation and Stream Ciphers	Functions	
7.	Public Key Cryptography and RSA	Strings	**Lab 2 is due** Lab 3
8.	Midterm		
9.	Other Public-Key Cryptosystems	Lists and Dictionaries	Lab 4 **Lab 3 is due**
10.	Project Proposal		
11.	Cryptographic Hash Functions	Classes/Exceptions	**Lab 4 is due**
12.	Message Authentication Codes	Sorting and Searching Algorithms	
13.	Digital Signatures	Plotting	
14.	Key Management and Distribution		
15.	Project Presentation		
16.	Final		

D. Evaluation

Final grade will be based on the following:

Lab 1 5%

Lab 2 5%

Lab 3 5%

Lab 4 5%

Mid Term 15%

Assignments 25%

Attendance 5%

Project 20%

Final 15%

E. Textbook

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

Laboratory

a. Hands-On Cryptography with Python; Leverage the power of Python to encrypt and decrypt data by Samuel Bowne
b. Programming in Python 3 with zyLab Authors Bailey Miller / CSE Ph.D., Univ. of California, Riverside / zyBooks (Former software engineer at SpaceX)
    i. **Sign in or create an account at learn.zybooks.com**
    ii. **Enter zyBook code: UDCCSCI455OladunniFall2019**
    iii. **Subscribe**

F. 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.

G. 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.