STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

# MASTER SYLLABUS

# CITA 360 - Cryptology in Theory and Practice

**Created by: Robert House**
**Updated by: Minhua Wang**

**CANINO SCHOOL OF ENGINEERING TECHNOLOGY**
**DECISION SYSTEMS**
**FALL 2018**

A. **TITLE**: Cryptology in Theory and Practice

B. **COURSE NUMBER:** CITA 360

C. **CREDIT HOURS: (Hours of Lecture, Laboratory, Recitation, Tutorial, Activity)**

**# Credit Hours:** 3
**# Lecture Hours:** 3 **per week**
**# Lab Hours:** **per week**
**Other:** **per week**

**Course Length:** 15 **Weeks**

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

F. **SEMESTER(S) OFFERED:** Spring

G. **COURSE DESCRIPTION:** This course provides a background in the characteristics of different cryptologic schemes. It introduces students to protocols and key establishment methods required for certificates and public key infrastructure.

H. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): CITA 165 Survey of Cybersecurity or CITA 220 Data ! Communications and Network Technology !
b. Co-requisite(s): none
c. Pre- or co-requisite(s): none

I. **STUDENT LEARNING OUTCOMES:**

By the end of this course, the student will be able to:

| ***Course Student Learning Outcome [SLO]*** | ***PSLO*** | ***ISLO*** |
|---|---|---|
| a. Outline the history of cryptology | 5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures | 5 |
| b. Compare and contrast the characteristics of different cryptologic schemes, including AES, DES, 3DES, RSA, Diffie-Hellman key exchange, and hash algorithms | 3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks | 5 |
| c. Compose protocols and key establishment methods, including certificates and public key infrastructure | 5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures | 2[CA]<br>5 |

| | | |
|---|---|---|
| d. Prepare applications of lightweight ciphers for RFIDs and mobile devices | 5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures | 5 |

**J. APPLIED LEARNING COMPONENT:** **Yes__X___ No_______**

- Classroom/Lab

**K. TEXTS:** None

**L. REFERENCES:** Various online resource such as SUNY Canton Library Books24x7 ITPro Book Database

**M. EQUIPMENT:** Computer lab classroom

**N. GRADING METHOD:** A-F

**O. SUGGESTED MEASUREMENT CRITERIA/METHODS:**

- Exams
- Assignments

**P. DETAILED COURSE OUTLINE:**

I. Introduction to Cryptography and Data Security.
   A. Symmetric Cryptography.
   B. Cryptanalysis.
   C. Modular Arithmetic.

II. Stream Ciphers.
   A. Encryption and Decryption with Stream Ciphers.
   B. Random Numbers and an Unbreakable Stream Cipher.

III. Data Encryption Standard (DES).

IV. Advanced Encryption Standard (AES).
   A. Overview of the AES Algorithm.
   B. Galois Fields.
   C. Internal Structure of AES.
   D. Decryption.
   E. Implementation in Software and Hardware.

V. Block Ciphers and Modes of Operation. !

VI. Introduction to Public-Key Cryptography.
   A. Symmetric vs. Asymmetric Cryptography.
   B. Practical Aspects of Public-Key Cryptography.
   C. Essential Number Theory for Public-Key Algorithms.

VII. The RSA Cryptosystem.
   A. Introduction
   B. Encryption and Decryption.
   C. Key Generation and Proof of Correctness.

VIII. Public-Key Cryptosystems.
   A. Diffie–Hellman Key Exchange.
   B. The Discrete Logarithm Problem.
   C. Security of the Diffie–Hellman Key Exchange.

IX. Digital Signatures.
   A. Principles of Digital Signatures.
   B. The RSA Signature Scheme.

X. Hash Functions.
   A. Security Requirements of Hash Functions.
   B. Overview of Hash Algorithms.
   C. The Secure Hash Algorithm SHA-1.

XI. Message Authentication Codes (MACs).

XII. Key Establishment.
   A. Key Freshness and Key Derivation.
   B. The $n^2$ Key Distribution Problem.
   C. Key Establishment Using Symmetric-Key Techniques.
   D. Key Establishment Using Asymmetric Techniques.

**Q. <u>LABORATORY OUTLINE</u>:** N/A !