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

MASTER SYLLABUS

CYBR360 - Cryptology in Theory and Practice

Created by: Kambiz Ghazinour

SCHOOL OF SCIENCE, HEALTH & CRIMINAL JUSTICE
FALL 2020

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

B. **COURSE NUMBER:** CYBR360

C. **CREDIT HOURS:** 3

- 3 hours of lecture per week
- Course length: 15 weeks

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** None

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

G. **COURSE DESCRIPTION:** This course provides a background in the characteristics of different cryptologic schemes. It introduces students to symmetric, asymmetric encryption models and protocols.

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

a. Pre-requisite(s): CYBR 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. Compare and contrast the characteristics of different cryptologic schemes, including AES, DES, RSA, Diffie-Hellman key exchange, and hash algorithms	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. Use cryptanalytic techniques to decode text encrypted with classical techniques	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 3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
c. Calculate the necessary key length to provide the required security in cryptographic and security applications	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 3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5

d. Use hashing applications and digital signature schemes	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 3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
e. Design and implement cryptographic systems	3. Use a variety of computer hardware and software and other technological tools appropriate and necessary for the performance of tasks	5
f. Evaluate peer viewpoints and provide constructive critiques to further the discussion.	1. Communicate clearly, concisely, and correctly in the written, spoken, visual, and electronic form that fulfills the purpose and meets the needs of audiences 2. Interpret, produce, and present work-related documents and information effectively and accurately	5

.

J. APPLIED LEARNING COMPONENT: **Yes**__X___ **No**_____

- Computer Lab Classroom

K. TEXTS: Paar, Christof, and Pelzl, Jan, Understanding Cryptography, Springer, 2010, ISBN 978-3-642-04100-6 or 978-3-642-04101-3
Textbook website: http://www.crypto-textbook.com/

L. REFERENCES: Various online resource such as SUNY Canton Library Books24x7 ITPro Book Database, Blackboard slides. All Power Point presentations are created by myself and are intended for use in this course.

M. EQUIPMENT: Computer lab classroom

N. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

- Participation
- Discussions
- Assignments
- Tests

P. DETAILED COURSE OUTLINE:

- Introduction to Cryptography and Data Security
  - Overview of Cryptology
  - Symmetric Cryptography
    - Basics
    - Simple Symmetric Encryption: The Substitution Cipher
  - Cryptanalysis
    - General Thoughts on Breaking Cryptosystems
    - How Many Key Bits Are Enough?
  - Modular Arithmetic and More Historical Ciphers
    - Modular Arithmetic
    - Integer Rings
    - Shift Cipher (or Caesar Cipher)
    - Affine Cipher
- Stream Ciphers
  - Introduction
    - Stream Ciphers vs. Block Ciphers
    - Encryption and Decryption with Stream Ciphers
  - Random Numbers and an Unbreakable Stream Cipher
    - Random Number Generators
    - The One-Time Pad
    - Towards Practical Stream Ciphers
  - Shift Register-Based Stream Ciphers
    - Linear Feedback Shift Registers (LFSR)
    - Known-Plaintext Attack Against Single LFSRs
- The Data Encryption Standard (DES) and Alternatives
  - Introduction to DES
    - Confusion and Diffusion
  - Overview of the DES Algorithm
  - Internal Structure of DES
    - Initial and Final Permutation
    - The f-Function
    - Key Schedule
  - Decryption
  - Security of DES
    - Exhaustive Key Search
    - Analytical Attacks
  - Implementation in Software and Hardware
  - DES Alternatives
    - The Advanced Encryption Standard (AES) and the AES Finalist Ciphers
    - Triple DES (3DES) and DESX
    - Lightweight Cipher PRESENT
- The Advanced Encryption Standard (AES)
  - Introduction
  - Overview of the AES Algorithm
  - Some Mathematics: A Brief Introduction to Galois Fields
    - Existence of Finite Fields
    - Prime Fields
    - Extension Fields GF(2m)
    - Addition and Subtraction in GF(2m)
    - Multiplication in GF(2m)
    - Inversion in GF(2m)
  - Internal Structure of AES
    - Byte Substitution Layer

        - Diffusion Layer
        - Key Addition Layer
        - Key Schedule
    - Decryption
    - Implementation in Software and Hardware
- More About Block Ciphers
    - Encryption with Block Ciphers: Modes of Operation
        - Electronic Codebook Mode (ECB)
        - Cipher Block Chaining Mode (CBC)
        - Output Feedback Mode (OFB)
        - Cipher Feedback Mode (CFB)
        - Counter Mode (CTR)
        - Galois Counter Mode (GCM)
    - Exhaustive Key Search Revisited
    - Increasing the Security of Block Ciphers
        - Double Encryption and Meet-in-the-Middle Attack
        - Triple Encryption
        - Key Whitening
- Introduction to Public-Key Cryptography
    - Symmetric vs. Asymmetric Cryptography
    - Practical Aspects of Public-Key Cryptography
        - Security Mechanisms
        - The Remaining Problem: Authenticity of Public Keys
        - Important Public-Key Algorithms
        - Key Lengths and Security Levels
    - Essential Number Theory for Public-Key Algorithms
        - Euclidean Algorithm
        - Extended Euclidean Algorithm
        - Euler's Phi Function
        - Fermat's Little Theorem and Euler's Theorem
- The RSA Cryptosystem
    - Introduction
    - Encryption and Decryption
    - Key Generation and Proof of Correctness
    - Encryption and Decryption: Fast Exponentiation
    - Speed-up Techniques for RSA
        - Fast Encryption with Short Public Exponents
        - Fast Decryption with the Chinese Remainder Theorem
    - Finding Large Primes
        - How Common Are Primes?
        - Primality Tests
    - RSA in Practice: Padding
    - Attacks
    - Implementation in Software and Hardware
- Public-Key Cryptosystems Based on the Discrete Logarithm Problem
    - Diffie–Hellman Key Exchange
    - Some Algebra
        - Groups
        - Cyclic Groups
        - Subgroups
    - The Discrete Logarithm Problem
        - The Discrete Logarithm Problem in Prime Fields
        - The Generalized Discrete Logarithm Problem
        - Attacks Against the Discrete Logarithm Problem
    - Security of the Diffie–Hellman Key Exchange
    - The Elgamal Encryption Scheme

        - From Diffie–Hellman Key Exchange to Elgamal Encryption
        - The Elgamal Protocol
        - Computational Aspects
        - Security
- Elliptic Curve Cryptosystems
    - How to Compute with Elliptic Curves
        - Definition of Elliptic Curves
        - Group Operations on Elliptic Curves
    - Building a Discrete Logarithm Problem with Elliptic Curves
    - Diffie–Hellman Key Exchange with Elliptic Curves
    - Security
    - Implementation in Software and Hardware
- Digital Signatures
    - Introduction
        - Odd Colors for Cars, or: Why Symmetric Cryptography Is Not Sufficient
        - Principles of Digital Signatures
        - Security Services
    - The RSA Signature Scheme
        - Schoolbook RSA Digital Signature
        - Computational Aspects
        - Security
    - The Elgamal Digital Signature Scheme
        - Schoolbook Elgamal Digital Signature
        - Computational Aspects
        - Security
    - The Digital Signature Algorithm (DSA)
        - The DSA Algorithm
        - Computational Aspects
        - Security
    - The Elliptic Curve Digital Signature Algorithm (ECDSA)
        - The ECDSA Algorithm
        - Computational Aspects
        - Security
- Hash Functions
    - Motivation: Signing Long Messages
    - Security Requirements of Hash Functions
        - Preimage Resistance or One-Wayness
        - Second Preimage Resistance or Weak Collision Resistance
        - Collision Resistance and the Birthday Attack
    - Overview of Hash Algorithms
        - Dedicated Hash Functions: The MD4 Family
        - Hash Functions from Block Ciphers
    - The Secure Hash Algorithm SHA-3
        - Preprocessing
        - Hash Computation
        - Implementation

Q. LABORATORY OUTLINE: N/A