COMP 4210 INTRODUCTION TO CRYPTOGRAPHY(3 credit hours)

Elmira College

SPRING 2025

Required Text:
Christof Paar, Jan Pelzl, Bart Preneel(2014). ***Understanding Cryptography: A Textbook for Students and Practitioners*** (2010th ed.). Springer.
Supplemental readings might be included to illustrate or expand on textbook readings.

Pre-requisites: MATH 3006 Abstract Algebra

Course Description

This is an introductory course designed to provide students with a comprehensive understanding of the fundamental concepts and techniques in cryptography. It covers classical cryptosystems, modern cryptographic algorithms, the RSA cryptosystem, pseudo-random sequence, Zero-Knowledge (ZK) proofs, and the ethical and social implications of cryptography. Students will gain hands-on experience through practical assignments and will be introduced to the mathematical underpinnings of cryptographic systems.

Course Objectives and Goals

- Understand the historical development and principles of classical and modern cryptographic systems.
- Apply cryptographic algorithms to secure data transmission and storage.
- Analyze and evaluate the security of cryptographic protocols.
- Generate pseudo-random sequences and understand their applications in cryptography.
- Discuss the ethical and social implications of cryptography in the digital age.
- Solve basic number-theoretic problems relevant to cryptography.

Evaluation of Performance

Your grade will be based upon your performance on exams, assignments, and participation.

Quizzes	30%
Assignments	30%
Midterm Exam	15%
Final Exam	25%
Total	100%

Grades will be assigned as follows:

A	93% and above	B-	80 - 82%	D+	67 - 69%
A-	90 - 92%	C+	77 - 79%	D	63 - 66%
B+	87 - 89%	C	73 - 76%	D-	60 - 62%

B	83 - 86%	C-	70 - 72%	F	59% or below

Withdrawal Policy: Please see Elmira College Bulletin for information on this policy.

Academic Honesty: Please read the section on Academic Honesty in the **Code of Conduct**. Briefly, academic dishonesty includes: cheating, fabrication, facilitating academic dishonesty, and plagiarism. Ask if you have any questions on whether something constitutes as academic dishonesty. All work must be original and new. Past assignments from current or other courses will not be accepted. Academic dishonesty will not be tolerated. It will result in zero on the assignment, and a report will be filed with the school. Continued practice will result in failure of the class. Institutional penalties may also apply with repeated acts of academic honesty.

Student Responsibility:

- It is your responsibility to keep track of assignments and due dates.
- You should ask questions concerning assignments and lectures, if you need any clarifications.
- If you are struggling in class, have concerns, and/or unsure about expectations, please stop by during office hours or make an appointment for another time.

Tentative Schedule of Topics

Topic	Materials	Tasks & Evaluations
Introduction to Cryptography and Data Security: Symmetric Cryptography; Cryptanalysis; Modular Arithmetic and More Historical Ciphers	Chapter 1	
Stream Ciphers: Random Numbers and an Unbreakable Stream Cipher; Shift Register-Based Stream Ciphers	Chapter 2	Assignment 1
The Data Encryption Standard (DES) and Alternatives: Introduction; Internal Structure; Decryption	Chapter 3	
Security of DES; Implementation; DES Alternatives	Chapter 3	Quiz 1
The Advanced Encryption Standard: Introduction;the AES Algorithm; A Brief Introduction to Galois Fields	Chapter 4	
Internal Structure of AES; Decryption; Implementation	Chapter 4	Assignment 2
Encryption with Block Ciphers: Modes of Operation	Chapter 5	
Increasing the Security of Block Ciphers	Chapter 5	Quiz 2
Introduction to Public-Key Cryptography: Symmetric vs. Asymmetric Cryptography; Practical Aspects	Chapter 6	
Essential Number Theory for Public-Key Algorithms	Chapter 6	Assignment 3
The RSA Cryptosystem: Introduction; Encryption and Decryption; Key Generation and Proof of Correctness	Chapter 7	
Speed-up Techniques for RSA; Finding Large Primes; RSA in Practice	Chapter 7	Midterm Exam
Public-Key Cryptosystems Based on the Discrete Logarithm Problem:Diffie–Hellman Key Exchange; Algebra	Chapter 8	
The Discrete Logarithm Problem; The Elgamal Encryption Scheme	Chapter 8	Assignment 4

Elliptic Curve Cryptosystems	Chapter 9	Quiz 3
Digital Signatures: The RSA Signature Scheme; The Elgamal Digital Signature Scheme	Chapter 10	
The Digital Signature Algorithm; The Elliptic Curve Digital Signature Algorithm	Chapter 10	Assignment 5
Hash Functions	Chapter 11	Quiz 4
Message Authentication Codes (MACs)	Chapter 12	
Key Establishment	Chapter 13	Assignment 6
Pseudo-random Sequence	Chapter 14	
Zero-Knowledge (ZK) Proofs	Chapter 15	Quiz 5
The Dolev-Yao Model	Chapter 16	
Ethical and Social Implications	Chapter 17	Final Exam