Course: EEGR 482 – Introduction to Cryptography

Faculty Name: Dr. Otily Toutsop

Term: Spring 2026

EEGR 482 - Introduction to Cryptography

Spring 2026

Credits: 3

Instructor: Dr. Otily Toutsop
Class: In-person
Email: otily.toutsop@morgan.edu/ottou1@morgan.edu
Office Hours: Online/in-person (Tuesday 4-5 pm or upon request)

Course Objectives:

- Three hours lecture; 3 credits. This course will provide practical knowledge of a wide range of cryptography mechanisms and explore their relationship with today's modern communications and networks. It includes the fundamentals of cryptography, classic and modern encryption, decryption, public and private key structures, digital signature, and secure hash functions. The course combines basic and technical cybersecurity ideas to show how cryptography fits into the bigger picture of designing, building, and protecting secure systems.
- Prerequisite: EEGR 317. Students must pass EEGR 317 with a grade of "C" or better.
- This course is structured Module wise where each module covers a specific concept and related activities (lecture slides, lecture videos, external YouTube videos and web links, quizzes, assignments, etc.) within one to few weeks.

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

- Identify the elements of a cryptographic system.
- Describe the differences between symmetric and asymmetric algorithms.
- Describe which cryptographic protocols, tools, and techniques are appropriate for a given situation.
- Describe how crypto can be used, its strengths and weaknesses, modes, and issues that must be addressed before implementation (e.g., key management).
- Describe and explain the fundamental concepts, technologies, components and issues related to communications and data networks.
- Apply and demonstrate knowledge of networking concepts
- Explain how various cryptographic algorithms and protocols work.
- Explain the application of cryptography in SSL, virtual private networks, etc.
- Evaluate a cryptosystem and explain its vulnerability to errors or attacks.
- Discuss the rules, laws, policies, and Ethics.
- Examine concepts of privacy and confidentiality.
- Describe approaches individuals, organizations, and governments have taken to protect privacy.

Course Content

Topics to be covered include: today's modern communications and networks. It includes the fundamentals of cryptography, classic and modern encryption, decryption, public and private key structures, digital signature, and secure hash functions.

Recommended Texts:

As this is an emerging field, there has yet to be a single good textbook for it. The following books are recommended:

"Cryptography and Network Security: Principles and Practice"

- **Authors:** William Stallings
- **Description:** This book provides a comprehensive introduction to the theory and practice of cryptography and network security. It covers various cryptographic algorithms, protocols, and their applications in network security.

Title: "Handbook of Applied Cryptography"

Authors: Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone

More resources will also be shared throughout the semester. Please check your canvas regularly.

Lecture Format: The lectures are meant to clarify and explain in an easy way some of the more difficult concepts presented in the text. The lectures are derived from the text and additional handouts. Therefore, the assigned readings are essential supplements to the lectures, and you are *expected* to read them. You are encouraged to explore other sources to supplement the lecture.

Quiz/Exam Policy:

- Quizzes will be administered using Canvas. An accessibility period and a time limit will be strictly enforced for the quizzes. **It is a student's responsibility to ensure that they can access Canvas to take the quizzes**.
- There will be **NO makeup quizzes**. Makeup exams are rarely given and only in the most extenuating cases. Students must provide an authorized (legitimate) excuse before a makeup exam can be considered.
- Exams (Midterm and Final) also will be administered using Canvas. Some questions may take the form of multiple choice and others will require you to provide answers to the questions.
- **Any instance of cheating will result in a score of '0' for the exam.**

Assignments/Projects:

There will be several assignments (HomeWorks) and a Final project at the end of the semester, which will be posted on different Canvas modules with appropriate instructions and due dates.
Please note the following guidelines for producing assignment in this course.

• All assignments must be submitted as a file (e.g.within the due date as specified in Canvas modules. The file should be named as follows: o Assignment Name (e.g., HW1)
o Your Last Name (e. xyz)
o Student ID

For example, a possible format for Assignement1 is, HW1_otily_001122

Evaluation Scheme:

The following table illustrates the components of the course and their corresponding weights (%).

Component	Percent
Assignments	**40**
Quizzes	**10**
Midterm Exam	**20**
Final Exam/Project	**25**
Attendance/Discussions	**5**

Grading Scale:

Grading will be based on a scale of 100 points broken down as follows:

90 - 100 = A
80 - 89 = B
70 - 79 = C
60 - 69 = D
0 - 59 = F

Canvas: In addition to the textbooks and study guide, the students be required to use Canvas learning management system. canvas will contain examples, practical questions, lecture outlines, websites for additional help and information, and exam/quiz/and laboratory grades.

WEEKS LECTURE TOPICS

Weeks	Module Topics	Labs / Assignments Due	KU Alignment
Week 1	Foundations of Cryptography & Security Services	HW1: Security Concepts	BCY
Week 2	Classical Cryptography	Lab 1: Classical Cipher Implementation	BCY
Week 3	Symmetric Key Cryptography (AES, DES, Modes)	HW2: AES Analysis	BCY
Week 4	Asymmetric Cryptography (RSA, Diffie-Hellman, ECC intro)	Lab 2: RSA Implementation	BCY
Week 5	Hash Functions & MACs	HW3: Hash & HMAC Security	BCY

Week 6	Digital Signatures & Authentication Protocols	Lab 3: Digital Signature Verification	BCY
Week 7	Public Key Infrastructure (PKI) & Certificate Management	Midterm Exam	BCY, ACR-O
Week 8	Cryptographic Protocols (SSL/TLS, IPSec)	Lab 4: TLS Analysis	BCY, ACR-O
Week 9	Mathematical Foundations (Modular Arithmetic, Finite Fields)	HW4: Number Theory	BCY, ACR-O
Week 10	Cryptanalysis Techniques	Lab 5: Cryptanalysis Exercise	BCY, ACR-O
Week 11	Wireless Sensor Networks Security, WSN architecture, Resource constraints & lightweight crypto, Key distribution in WSN, IoT cryptographic vulnerabilities, Secure routing & data aggregation	WSN Security Mini-Project Assigned	WSN, BCY
Week 12	Privacy, Legal & Ethical Issues in Cryptography & IoT	Legal/Privacy Analysis Paper Due	PRI-O, HOF-O
Week 13	Secure Implementation & Security Best Practices (Side-channel risks, key lifecycle management, embedded crypto)	Lab 6: Secure Key Management	BCY, ACR-O, WSN
Week 14	Final Project Presentations (Cryptographic System Design or WSN Security Case Study)	Final Project Submission	BCY, ACR-O, PRI-O, WSN