Title: *Introduction to Cryptography and Security: ECE 6280*

Semester: *Fall 2026*

CRN(s):

Instructors: Dr. Paul Voss = Metz (paul.voss@ece.gatech.edu)

Class times : Tu 5 :00-6 :15 pm / Th 3:30 – 4:45 pm

Office Hours: Tu 6:15 pm – 7:15 pm & by appointment

Course Overview

To provide:
1) An introduction to practical issues in information security
2) An in-depth mathematical introduction to basic cryptographic primitives including:
a. Block and stream ciphers
b. Public key cryptosystems
c. Digital signatures
d. Hash functions
e. Key agreement
f. Authentication
3) Development of skill in combining primitives

SPIs

COURSE	**ECE 6280 Cryptography and Secure Communications**	**Indicator for evaluation**
TIG	DSP	
Outcome 1	SPI 1.1: Demonstrate knowledge of the fundamental modular mathematics, and analysis of attacks against cryptographic primitives.	HW and Exams
	SPI 1.2: Demonstrate the ability to analyze the security of cryptographic protocols that combine cryptographic primitives.	HW and Exams
Outcome 2	SPI 2.1: Students will be able to build cryptographic systems and identify security considerations	Project
Outcome 3	SPI 3.1: Students will be able to use research literature and updated	Assignments and Tests

	standards documentation to demonstrate understanding of evolution of cryptographic protocols and primitives.	

Learning Outcomes

By the end of this course, students should be able to:

- Demonstrate ability to use modular mathematics to solve cryptography problems.
- Analyze the security of a cryptographic primitive
- Combine cryptographic primitives to build a cryptographic system
- Use research literature to understand the security of new protocols and cryptographic systems
- Explain clearly the security considerations that have gone into the design of the most popular primitives and protocols.

Textbook (should procure a copy)

Cryptography - Theory and Practice, 4th Edition, by Douglas R.
Stinson, JCRC press.

Prerequisites

instructor approval. Graduate Standing. Undergraduates allowed to take course with instructor permission

Grading

Graded Homework	20%
Projects	25%
Exams (15% each)	30%
Final Project	25%

Grading Policy

Your final grade will be assigned as a letter grade according to the following scale:
A 90-100%
B 80-89%
C 70-79%
D 60-69%
F 0-59%
Homework and Projects are due by midnight on due date. Late Homework and Projects receive a 50% penalty.

Day	Date	Topic	Reading	Assignment
Thu	Aug 27	Introduction and Historical Cryptography	Stinson Chapters 1 & 2	
Tue	Sep 1	Cryptography and Computational Complexity 1	Impagg	
Thu	Sep 3	Cryptography and Computational Complexity 2		
Tue	Sep 8	More Computational Complexity, Shannon Theory for Cryptography		
Thu	Sep 10	Block Cipher Theory: Linear and Differential Attacks		HW 1 Due
Tue	Sep 15	Block Cipher Practice: DES, 3DES, AES,		
Thu	Sep 17	Stream Cipher Theory: Statistical and Algebraic Attacks		Proj 1 Due
Tue	Sep 22	Stream Ciphers in Practice: ChaCha20		
Thu	Sep 24	Mathematical Preliminaries		HW 2 Due
Tue	Sep 29	RSA #1: Primality Testing, non-factoring attacks		
Thu	Oct 1	RSA #2: Factoring		Proj 2 Due

Tue	Oct 6	RSA #3: Factoring (analysis of quadratic sieve, mention of number field sieve)		
Thu	Oct 8	RSA #4: Practice		HW 3 Due
Tue	Oct 13	Discrete Log Cryptosystems: Theory & Attacks		
Thu	Oct 15	Polynomial Field DL: Theory & Attacks		HW 4 Due
Tue	Oct 20	Elliptic Curve DL: Theory		
Thu	Oct 22	Elliptic Curve Practice: Choosing a curve, standards , Digital Signature #1: RSA based theory & Practice,		Proj 3 Due
Tue	Oct 27	Fall Break: No Class		
Thu	Oct 29	Fall Break: No Class		
Tue	Nov 3	Test 1		Test 1 (covers material up to, but not including Digital Signatures)
Thu	Nov 5	Digital Signature #2: ECC Practice		
Tue	Nov 10	Hash Function Theory & Practice: Message Authentication Codes, SHA2, SHA3	Stinson 4.1-4.3	HW 5 Due

Thu	Nov 12	Post Quantum Cryptography Overview	Stinson 4.4-4.5	
Tue	Nov 17	Key Distribution, Key Agreement	Stinson 9	
Thu	Nov 19	Identity Authentication, Digital Certificates in Practice, Protocol Practice: TLS & VPN implementation	Stinson 10-12	HW 6 Due
Tue	Nov 24	Supplementary Material: Cryptocurrency		
Thu	Nov 26	Supplementary Material: Cryptocurrency		
Tue	Dec 1	Supplementary Material: Recent Research		Final Project Due
Thu	Dec 3	Protocol Analysis		
Tue	Dec 8	Review		
	TBA	Final Exam		Final Exam

Academic Integrity

Academic honesty is essential to achieve high-quality education and to maintain the value of a Georgia Tech diploma. While I encourage you to work together and to form study groups, it is important that you take responsibility for the content of all assignments. Collaboration is allowed on homework. Cheating on quizzes, tests, and final exams will not be tolerated. When uncovered, violations will be reported to the Office of Student Integrity and the assignment grade becomes 0. If students have questions, a valuable resource is the Georgia Tech Student Code of Conduct and the Academic Honor Code.

An AI policy is in the works for this course. For now, please defer to your instructors approved use and expectations on using AI for this course. Any AI use should be meet institute policies listed on this Office of Information and Technology page AND the Student Code of Conduct. Instructors have the ability to

adjust their AI policies within courses for future assignments if issues arise by clearly announcing them in writing to the students. Instructors may not retroactively change policies for former assignments.

SUPPORT SERVICES AND RESOURCES

In your time at Georgia Tech, you may find yourself in need of support. Below you will find some resources to support you both as a student and as a person.

Academic Support

- Center for Academic Success
    - Academic Coaching
- Office of Undergraduate Education's Learning Assistance Program
    - 1-to-1 tutoring
    - Peer-Led Undergraduate Study (PLUS)
    - Drop-in tutoring
- Communication Center - Individualized help with writing and multimedia projects

Academic advisors for your major

Personal Support

Georgia Tech Resources

- See Prof. Voss (GTE Dean of Students Representative), room 221 to see what can be done at GTE in case of crisis. In a crisis call the GTE urgent support phone: 00 33 3 54 84 61 00
- The Office of the Dean of Students | **404-894-2565** | 2nd floor, Smithgall Student Services Building; You also may request assistance here
    - In the event of an after-hours emergency, individuals should contact the Georgia Tech Police Department at **(404) 894-2500** and request that the "Dean on Call" be contacted. There is an emergency "Dean on Call" at all times to assist students in need.