

Undergraduate Course Syllabus

MAT 260: Cryptology

Course Prerequisites

None

Course Description

Cryptology is a mathematically rich subject that includes both cryptography - the science of making secret codes - and cryptanalysis - the science of breaking secret codes. Historically, cryptology has played a central role in military and government covert actions and modern- day data security. In this course, we develop a number of mathematical topics including modular arithmetic, statistics, probability, permutation functions, algorithms, binary numbers, base twenty-six, primes, factorization, the Euclidean algorithm, and Fermat's Little Theorem as they pertain to classical cryptographic techniques, symmetric computer-based cryptography, and public key cryptography. We also examine the historical backdrop of cryptology and examine legal issues concerning cryptology.

Course Outcomes

- Investigate properties of modular arithmetic, statistics, probability, permutation functions, algorithms, binary numbers, base 26, primes, factorization, the Euclidean algorithm, and Fermat's little theorem as they pertain to classical cryptographic techniques, symmetric computer-based cryptography, and public key cryptography
- Discuss the historical backdrop to the subject of cryptology
- Examine legal issues concerning cryptography

Required Materials

Using your learning resources is critical to your success in this course. Please purchase directly through the [SNHU Online Bookstore](#) rather than any other vendor. Purchasing directly from the bookstore ensures that you will obtain the correct materials and that the IT Service Desk, your advisor, and the instructor can provide you with support if you have problems.

Introduction to Cryptography With Coding Theory

Wade Trappe, Lawrence C. Washington

3rd Edition 2021

Pearson Education

MBS Direct SKU# 9410617

Technical Requirements

Make sure you've met the [technical requirements](#) to complete this course.

Diversity, Equity, and Inclusion

As indicated in our core values, SNHU is committed to “embrace diversity where we encourage and respect diverse identities, ideas, and perspectives by honoring difference, amplifying belonging, engaging civilly, and breaking down barriers to bring our mission to life.”

This may or will be reflected in SNHU’s curriculum as we embrace and practice diversity, equity, and inclusion (DEI) to provide the most transformative experience for our students, faculty, and staff. Because topics pertaining to DEI can be sensitive, please remember that embodying and practicing diversity, equity, and inclusion is one of our core values that you will encounter throughout the academic experience. In higher education, we are expected to think and engage critically. Use a growth mindset to embrace the diverse readings, course assignments, and experiences of your peers and faculty.

For more information about DEI at SNHU, please visit our website at the [Office of Diversity and Inclusion](#).

Instructor Availability and Response Time

Your class interaction with the instructor and your classmates will take place on a regular, ongoing basis. Your instructor will be actively engaged within the course throughout the week. You will normally communicate with your instructor in the weekly discussions or the General Questions discussion topic so that your questions and the instructor’s answers benefit the entire class. You should feel free, however, to communicate with your instructor via SNHU email at any time, particularly when you want to discuss something of a personal or sensitive nature. Your instructor will generally provide a response within 24 hours. Instructors will post grades and feedback (as applicable) within seven days of an assignment’s due date, or within seven days of a late submission.

Grade Distribution

Assignment Category	Number of Graded Items	Point Value per Item	Total Points
Discussions	7	20	140
Assignments	7	45	315
Reflection Paper	1	45	45
Milestone One	1	75	75
Milestone Two	1	100	100
Final Project	1	325	325
			Total Course Points: 1,000

This course may also contain non-graded activities. The purpose of these non-graded activities is to assist you in mastering the learning outcomes in the graded activity items listed above.

University Grading System: Undergraduate

Grade	Numerical Equivalent	Points
A	93–100	4
A-	90–92	3.67

Grade	Numerical Equivalent	Points
B+	87–89	3.33
B	83–86	3
B-	80–82	2.67
C+	77–79	2.33
C	73–76	2
C-	70–72	1.67
D+	67–69	1.33
D	60–66	1
F	0–59	0
I	Incomplete	
IF	Incomplete/Failure *	
IP	In Progress (past end of term)	
W	Withdrawn	

* Please refer to the [policy page](#) for information on the incomplete grade process.

Grading Guides

Specific activity directions, grading guides, posting requirements, and additional deadlines can be found in the Assignment Information section of the course.

Weekly Assignment Schedule

All readings can be found within each module of the course, and assignment instructions can be found in the Assignment Information section of the course. Assignments and discussion posts during the first week of each term are due by 11:59 p.m. Eastern Time. Assignments and discussion posts for the remainder of the term are due by 11:59 p.m. of the student's local time zone.

Module	Topics and Assignments
One	Classical Cryptosystems <i>Introduction to Cryptography With Coding Theory</i> , Chapter 1 (entire chapter) and Chapter 2 through section 2.7: Enigma 1-1 Discussion: The Relationship Between Cryptography and Mathematics 1-2 Create a MathWorks Account (Non-graded) 1-3 Assignment: Module One Problem Set 1-4 Final Project Review (Non-graded)
Two	Number Theory Basics and the One-Time Pad <i>Introduction to Cryptography With Coding Theory</i> , Chapter 3 through section 3.7: Primitive Roots, and Chapter 4 through section 4.4: Perfect Secrecy of the One-Time Pad 2-1 Discussion: Classic and Historical Ciphers 2-2 Assignment: Module Two Problem Set

Module	Topics and Assignments
Three	Stream and Block Ciphers <i>Introduction to Cryptography With Coding Theory</i> , Chapter 5 through section 5.3: RC4, and Chapter 6 (entire chapter) 3-1 Discussion: Stream and Block Ciphers 3-2 Practice Activity: Vigenère Cipher 3-3 Assignment: Module Three Problem Set 3-4 Milestone One: Historical Background and Properties
Four	The Data Encryption Standard (DES) <i>Introduction to Cryptography With Coding Theory</i> , Chapter 7 4-1 Discussion: Computational Complexity and Cryptology 4-2 Assignment: Module Four Problem Set
Five	The Advanced Encryption Standard (AES) and RSA Algorithm <i>Introduction to Cryptography With Coding Theory</i> , Chapters 8 and 9 5-1 Discussion: Mathematical Principles in Public Key Cryptology 5-2 Assignment: Module Five Problem Set 5-3 Milestone Two: Mathematical Analysis
Six	Hash Functions <i>Introduction to Cryptography With Coding Theory</i> , Chapter 11 (entire chapter) and Chapter 12 through section 12.4: Using Hash Functions to Encrypt 6-1 Discussion: Hash Functions 6-2 Assignment: Module Six Problem Set
Seven	Digital Signatures <i>Introduction to Cryptography With Coding Theory</i> , Chapters 13 and 14 7-1 Assignment: Module Seven Problem Set 7-2 Final Project Submission: Cryptosystem Analysis
Eight	Security Protocols <i>Introduction to Cryptography With Coding Theory</i> , Chapter 15 through section 15.7: SSL and TLS 8-1 Discussion: Legality and Privacy Concerns Related to Cryptology 8-2 Reflection Paper: Privacy and Information Security

Course Participation

Course participation is required within the first week of the term for all online courses. *Participation* in this context is defined as completing one graded assignment during the first week of the course. Otherwise, students will be administratively removed for nonparticipation. Students who do not participate during the first week may forfeit their rights to be reinstated into the course. Students who stop attending a course after the first week and who do not officially withdraw will receive a grade calculated based on all submitted and missed graded assignments for the course. Missed assignments will earn a grade of zero. See the [course withdrawal policy](#) and the [course participation policy](#) for further information.

Late Assignments

Students who need extra time may submit assignments (excluding discussion board postings) up to one week after the assignment due date. Discussion board submissions will not be accepted for credit after the deadline except in extenuating circumstances.

- A penalty of 10 percent of the total value of the assignment will be applied to the grade achieved on the late assignment regardless of the day of the week on which the work is submitted.
- Students who submit assignments more than one week late will receive a grade of zero on the assignment unless they have made prior arrangements with the instructor.

Students must submit all assignments no later than 11:59 p.m. (in their own time zone) on the last day of the term. No assignments are accepted after the last day of the term unless an incomplete has been submitted. See the [incomplete grades policy](#).

There may be times an instructor makes an exception to the late assignment policy. Instructors may accept late work, including discussion board posts, with or without prior arrangement.

- Exceptions to the late policy on these grounds are left to the instructor's discretion, including whether the late penalty is applied or waived. Students should not assume that they will be allowed to submit assignments after the due dates.
- If an instructor finds that they are unable to determine whether an exception to the late policy would be appropriate without documentation, the collection and review of student documentation should be handled through the Dispute Resolution team in order to protect the student's privacy. In these cases, students should file a [Student Concern Dispute form](#) to have the circumstances reviewed.

If a student is experiencing (or knows they will experience) a circumstance, including pregnancy, that is protected under the Americans with Disabilities Act or Title IX, they are encouraged to contact the [Online Accessibility Center \(OAC\)](#) as soon as possible to explore what academic accommodations might be offered. Instructors must honor all deadlines established through the OAC.

Student Handbook

Review the [student handbook](#).

ADA/504 Compliance Statement

Southern New Hampshire University (SNHU) is dedicated to providing equal access to individuals with disabilities in accordance with Section 504 of the Rehabilitation Act of 1973 and with Title III of the Americans with Disabilities Act (ADA) of 1990, as amended by the Americans with Disabilities Act Amendments Act (ADAAA) of 2008.

SNHU prohibits unlawful discrimination on the basis of disability and takes action to prevent such discrimination by providing reasonable accommodations to eligible individuals with disabilities. The university has adopted the [ADA/504 Grievances Policy](#) (version 1.2 effective October 16, 2017), providing for prompt and equitable resolution of complaints regarding any action prohibited by Section 504 or the ADA.

For further information on accessibility support and services, visit the [Disability and Accessibility Services](#) webpage.

Academic Integrity Policy

Southern New Hampshire University requires all students to adhere to high standards of integrity in their academic work. Activities such as plagiarism and cheating are not condoned by the university. Review the [full academic integrity policy](#).

Artificial Intelligence (AI) Usage Guidelines

We recognize there are a variety of generative AI programs available to assist in your work. Generative AI programs are not a replacement for human creativity, originality, or critical thinking. However, within limited circumstances, and with proper citation, generative AI may be used as a tool in this course.

For further guidance, review [this student guide to generative AI](#).

Copyright Policy

Southern New Hampshire University abides by the provisions of United States Copyright Act (Title 17 of the United States Code). Any person who infringes the copyright law is liable. Review the [full copyright policy](#).

Use of Open Educational Materials

Students may encounter openly licensed learning materials such as open access (OA) publications and open educational resources (OERs) in their courses. Southern New Hampshire University uses these openly licensed materials in compliance with the stated license terms on the material. Students must also ensure that any uses outside of this course follow the license terms of the material. The selection of these materials adheres to SNHU's accepted guidelines on course material adoption.

Use of Artificial Intelligence (AI) to Generate Content

This course may contain some material created with the help of AI tools. Any AI-generated content has been thoroughly vetted by a team of instructional designers, editors, subject matter experts, and deans. Revisions have been made to ensure accuracy and clarity.

Withdrawal Policy

Review the [full withdrawal policy](#).

Southern New Hampshire University Policies

More information about SNHU policies can be found on the [policy page](#).