Introduction to Cryptology
CDA 3101
Location: NEB, MWF 11-12:15
Academic Term: Summer 2025

Instructor:
Prof. Cheryl Resch
Cheryl.resch@ufl.edu

Teaching Assistants:
Bhanu Prakash Reddy Vangala (bvangala1@ufl.edu)
Anurag Yadav (anuragswar.yadav@ufl.edu)
Nanjie Rao (raon@ufl.edu)
Joel Hirschmann (joelhirschmann@ufl.edu)

Office Hours
Monday 1-2 pm MALA 4110
Wednesday 5-6 pm https://ufl.zoom.us/my/cherylresch

Discord
https://discord.gg/757ZGUxBpr

Course Description
Introduces classical and modern cryptography and cryptanalysis, including symmetric and asymmetric (public key) ciphers. Covers cryptographic hash functions, block and stream ciphers, and cryptanalysis. Reviews applications of cryptography, cryptographic standards and protocols.

Course Pre-Requisites / Co-Requisites
To take this course, you must have completed the following course:
- COT 3100

Course Student Learning Outcomes
By the end of this course, you will be able to:
- Demonstrate modulo arithmetic underlying cryptography
- Implement and analyze block and stream ciphers
- Perform encryption and key generation for public key cryptography systems
- Describe and use hash functions and message authentication codes
- Demonstrate the operation of identification and digital signature schemes
- Identify key establishment protocols and analyze common attack vectors
- Demonstrate knowledge of advanced cryptographic topics such as side channel attacks, elliptic curve cryptography, and secure communication protocols.

Materials and Supply Fees
None

Required Textbooks and Software
- Handbook of Applied Cryptography

    - https://cacr.uwaterloo.ca/hac/qemu
- GradeScope
- SEED Labs https://seedsecuritylabs.org/
- Google Colab https://colab.research.google.com/

Recommended Materials

- None

Weekly Course Schedule

Week 1 – Introduction
Week 2 – Mathematical foundations
Week 3 – Random number generation, stream ciphers
Week 4 – Block ciphers
Week 5 – Public key encryption
Week 6 – Hash functions
Week 7 – Authentication and identification
Week 8 – Digital Signature
Week 9 – Key establishment and key exchange
Week 10 – Side channel attacks and elliptic curve cryptography
Week 11 – IPSec and VPNs, Kerberos
Week 12 – Review

Class Expectations

Late Policy

Weekly assignments may be turned in one day late with a penalty of 50%.

Honesty Policy

Your code for your assignments must be your own. You may discuss assignments with others, but **copy/pasting code from other students or online resources is strictly prohibited**.
Your writing for assignments must be your own. **Copy/pasting writing from other students is strictly prohibited.**
You may not copy code from another student. You may not copy AI generated output. You may not copy code from the internet.
We will be using TurnItIn to check for plagiarism.
A sanction of an E in the course will be imposed if a student is found to have violated the honesty policy.

Discussion of Grades

Grades on any assignment may be discussed with me via email or in office hours up to **seven days after the grade was released**.

Evaluation of Grades

We will make every effort to have each assignment graded and posted within one week of the due date.

Course Grading Policy

Assignment	Points
Assignments (11, one drop)	80%
Final Assessment	20%
Total	**100%**

Grading Scale

Percent	Grade	Grade Points
93 - 100	A	4.00
90.0 - 92.99	A-	3.7
87 - 89.99	B+	3.3
83 - 86.99	B	3.00
80.0 - 82.99	B-	2.7
77 - 79.99	C+	2.3
73 - 76.99	C	2.00
70.0 - 72.99	C-	1.7
67 - 69.99	D+	1.3
63 - 66.99	D	1.00
60.0 - 63.99	D-	0.7
0 - 59.99	E	0.00

More information on UF grading policy may be found at:
https://catalog.ufl.edu/UGRD/academic-regulations/grades-grading-policies/

Students Requiring Accommodations

Students with disabilities who experience learning barriers and would like to request academic accommodations should connect with the disability Resource Center by visiting https://disability.ufl.edu/students/get-started/. It is important for students to share their accommodation letter with their instructor and discuss their access needs, as early as possible in the semester.

Course Evaluation

Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

University Honesty Policy

UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://sccr.dso.ufl.edu/process/student-conduct-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report

any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Commitment to a Safe and Inclusive Learning Environment

The Herbert Wertheim College of Engineering values varied perspectives and lived experiences within our community and is committed to supporting the University's core values, including the elimination of discrimination. It is expected that every person in this class will treat one another with dignity and respect regardless of race, creed, color, religion, age, disability, sex, sexual orientation, gender identity and expression, marital status, national origin, political opinions or affiliations, genetic information, and veteran status.

If you feel like your performance in class is being impacted by discrimination or harassment of any kind, please contact your instructor or any of the following:

- Your academic advisor or Graduate Program Coordinator
- HWCOE Human Resources, 352-392-0904, student-support-hr@eng.ufl.edu
- Pamela Dickrell, Associate Dean of Student Affairs, 352-392-2177, pld@ufl.edu
- Toshikazu Nishida, Associate Dean of Academic Affairs, 352-392-0943, nishida@eng.ufl.edu

Software Use

All faculty, staff, and students of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Student Privacy

There are federal laws protecting your privacy with regards to grades earned in courses and on individual assignments. For more information, please see: https://registrar.ufl.edu/ferpa.html

Campus Resources:

Health and Wellness

U Matter, We Care:

Your well-being is important to the University of Florida. The U Matter, We Care initiative is committed to creating a culture of care on our campus by encouraging members of our community to look out for one another and to reach out for help if a member of our community is in need. If you or a friend is in distress, please contact umatter@ufl.edu so that the U Matter, We Care Team can reach out to the student in distress. A nighttime and weekend crisis counselor is available by phone at 352-392-1575. The U Matter, We Care Team can help connect students to the many other helping resources available including, but not limited to, Victim Advocates, Housing staff, and the Counseling and Wellness Center. Please remember that asking for help is a sign of strength. In case of emergency, call 9-1-1.

Counseling and Wellness Center: https://counseling.ufl.edu, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Discrimination, Harassment, Assault, or Violence

If you or a friend has been subjected to sexual discrimination, sexual harassment, sexual assault, or violence contact the **Office of Title IX Compliance**, located at Yon Hall Room 427, 1908 Stadium Road, (352) 273-1094, title-ix@ufl.edu

Sexual Assault Recovery Services (SARS)

Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Connections Center, Reitz Union, 392-1601. Career assistance and counseling; https://career.ufl.edu.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall*,* 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://sccr.dso.ufl.edu/policies/student-honor-code-student-conduct-code/;https://care.dso.ufl.edu.

On-Line Students Complaints*:* https://distance.ufl.edu/getting-help/; *https://distance.ufl.edu/state-authorization-status/#student-complaint*.