Syllabus: CIS 4362 – Applied Cryptography

Course Information

- Course Number and Title: CIS 4362 – Applied Cryptography
- **Credit Hours:** 3 (Lecture Hours: 3, Lab Hour: 0)
- **Academic Term: Spring 2026**

Instructor Information

- **Instructor:** Xianping Wang
- **Office Location: B**ARC 1189
- **Office Hours**: TR 11AM-12:30PM
- **Other Ways to Contact You: Appointment through email xianpingwang@floridapoly.edu**

Course Details

- **Delivery Mode**: In-Person, Room – IST-1064, Tuesdays and Thursdays, 9:30 AM – 10:45 AM.
- **Official Catalog Course Description**: This course introduces cryptographic primitives and how they are implemented in applications. Topics covered include: symmetric key encryption algorithms, public key encryption, digital signatures, and message integrity. This course introduces cryptographic primitives and how they are implemented in applications. Topics covered include: symmetric-key encryption algorithms, public key encryption, digital signatures, and message integrity.
    - **Course Pre and/or Co-Requisites**:
        - STA 2023 - Statistics 1 or STA 3032 Probability and Statistics) and
        - COP 3530 - Data Structures & Algorithms or (COP 4415 - Data Structures and COP 4531 - Algorithm Design & Analysis
    - **Communication/Computation Skills Requirement (6A-10.030)**: N
- **Required Texts:**
    - **Cryptography and Network Security: Principles and Practice (8th Edition), by William Stallings**
    - **ISBN 10:1-292-15858-1, ISBN 13: 978-1-292-15858-7**
    - **Internet Security: A Hands-on Approach (3rd Edition) By Wenliang Du ISBN: 978-17330039-6-4**
-
    - **Equipment and Materials**: None
- **Course Objectives**:
    - To familiarize the students with the fundamental concepts of cryptographic primitives in the real-world applications.
    - To provide the opportunity to explore the standards of key-exchange protocols in the real-time communication network.
    - To enable the students to make a trade-off between security and performance in different cryptographic protection mechanisms.
    - To enable the students to develop their basic skill and to apply the acquired knowledge in the design and implementation of secure architectures.

- **Course Learning Outcomes**:
    - Describe the purpose of cryptography and list ways it is used in data communications.
    - Define the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plain text in cipher text.
    - Explain how public key infrastructure supports digital signing and encryption.
    - Describe real-world applications of cryptographic primitives and protocols.

- Summarize security definitions related to attacks on cryptographic primitives, including attacker capabilities and goals.

- **Alignment with Program Outcomes**:

Course Learning Outcome	Program Learning Outcomes	Learning Level
Describe the purpose of cryptography and list ways it is used in data communications.	1	Define
Define the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plain text in cipher text.	2	Demonstrate
Explain how public key infrastructure supports digital signing and encryption.	2	Understand
Describe real-world applications of cryptographic primitives and protocols.	3	Apply
Summarize security definitions related to attacks on cryptographic primitives, including attacker capabilities and goals.	4	Analyze

Academic Support Resources

- **Library**: Students can access the Florida Polytechnic University Library through the University website and Canvas, on and off campus. Students may direct questions to Academic Success Center success@floridapoly.edu or by email, library@floridapoly.edu.
- **Peer Learning Strategists**: These are specially trained student leaders who help their peers strategize approaches to course content and work through solution methods. PLS students work in collaboration with the courses they support so the content and methods are aligned with your instructors' expectations. The PLS room is located on the first floor of the IST in the center hallway.
- **Writing Center**: Located on the second floor of the IST (2059/2061), the Writing Center helps students to develop their writing and presentation skills. Consultations are available in person and virtually. For more detail, visit https://floridapolytechnic.libguides.com/writingservices.

Course Schedule

- This syllabus is tentative and may be subject to change. Everything in the syllabus might change except for 1) the Course Description; 2) the textbook; and 3) the grading policy.
- Assignments/Labs/Quizzes/Projects will vary in number and dates.
- Important Dates: https://floridapoly.edu/academics/academic-calendar/index.php

Week	Topic	Assignments
1	Basic Concepts	
2	Classical Encryption Techniques	
3	Information Theory, Complexity Theory, and Number Theory	Assignment 1 Quiz 1
4	Block Ciphers and the Data Encryption Standard	
5	Block Ciphers and the Data Encryption Standard	
6	Advanced Encryption Standard and Finite Fields	Assignment 2 Quiz 2
7	Advanced Encryption Standard and Block Cipher Operation	
8	Review Midterm	Assignment 3 Quiz 3
9	Spring Break, No class	
10	Public-Key Cryptography and RSA	
11	Public-Key Cryptography and RSA	
12	Other Public-Key Cryptosystems	Assignment 4 Quiz 4
13	Cryptographic Hash Functions	
14	Message Authentication Codes	
15	Digital Signatures, Key Management and Distribution	Assignment 5 Quiz 5

16	User Authentication Protocols	
17	Final Exams	

Course Policies

Attendance

- Students in courses are expected "to attend all of their scheduled University classes and to satisfy all academic objectives as defined by the instructor" (University Policy, FPU-5.0010AP).
- Exceptions to any attendance requirements may be made on a case-by-case basis.

Students Feeling Sick

Students should not come to class if they are feeling ill, particularly if experiencing symptoms of COVID-19, or if you have been directed by a health professional to quarantine. Students who are experiencing an emergency situation that aligns with an academic exercise of consequence (e.g./a Common Exam) should work with CARE Services at care@floridapoly.edu

Late Work/Make-up work

- To make up an exam and project presentation, signed document from authority (such as doctor, clinic, law enforcement officers, etc.) is needed.
- The penalty for late assignment is 10% per day. No late assignment will be accepted later than 3 days after the due date.
- *Other makeup work need approval from the instructor and request in advance.*

Grading Scale

A : above 93%
A− : 90% - 92%
B+ : 87% - 89%
B : 83% - 86%
B− : 80% - 82%
C+ : 77% - 79%
C : 73% - 76%
C− : 70% - 72%
D+ : 67% - 69%
D : 63% - 66%
D− : 60% - 62%
F : below 60%

Assignment/Evaluation Methods

Attendance: 5%
Quiz: 15%
Midterm Exam: 20%
Final Exam: 20%
Assignments/labs/projects: 40%

Total: 100%

University Policies

Reasonable Accommodations

The University is committed to ensuring equal access to all educational opportunities. The University, through the Office of Disability Services (ODS), facilitates reasonable accommodations for students with disabilities and documented eligibility. It is the student's responsibility to self-identify as a student with disabilities and register with ODS to request accommodations.

If you have already registered with ODS, please ensure that you have requested an accommodation letter for this course through the ODS student portal and communicate with your instructor about your approved accommodations as soon as possible. Arrangements for testing accommodations must be made in advance. Accommodations are not retroactive.
If you are not registered with ODS but believe you have a temporary health condition or permanent disability requiring an accommodation, please contact ODS as soon as possible.

The Office of Disability Services (ODS):
DisabilityServices@floridapoly.edu
(863)874-8770
The Access Point
ODS website: www.floridapoly.edu > Student Affairs > Health Wellness > Disability Services

Accommodations for Religious Observances, Practices and Beliefs

The University will reasonably accommodate the religious observances, practices, and beliefs of individuals in regard to admissions, class attendance, and the scheduling of examinations and work assignments. (See University Policy.)

Title IX

Florida Polytechnic University is committed to ensuring a safe, productive learning environment on our campus that prohibits sex discrimination and sexual misconduct, including sexual harassment, sexual assault, dating violence, domestic violence and stalking. It is important for you to know that there are resources available if you or someone you know needs assistance. You may speak to your professor, but your professors have an obligation to report the incident to the Title IX Coordinator. It is an educational goal that you feel able to share information related to your life experiences in classroom discussions and in one-on-one meetings. However, it is requirement for university employees to share information with the Title IX Coordinator regarding disclosure. However, please know that your information will be kept private to the greatest extent possible. You will not be required to share your experience. If you want to speak to someone who is permitted to keep your disclosure confidential, please seek assistance from the Florida Polytechnic University Ombuds Office, BayCare's Student Assistance Program, 1-800-878-5470 and locally within the community at Peace River Center, 863-413-2707 (24-hour hotline) or 863-413-2708 to schedule an appointment.

Academic Integrity

All students are expected to adhere to the highest standards of academic integrity. Violations of academic integrity include actions such as cheating, plagiarism, use of unauthorized resources, illegal use of intellectual property, and inappropriately aiding other students. Such actions undermine the central mission of the university and negatively impact the value of your Florida Poly degree. It is critical that students take a professional approach to their academic work. The faculty and administration take academic integrity very seriously. Suspected violations will be fully investigated, possibly resulting in an academic integrity hearing and sanctions against the accused student if found in violation. Sanctions range from receiving a zero on the exam or assignment, to expulsion from the university. Repeat offenders are subject to more severe sanctions and penalties. Do not compromise your integrity for a perceived short-term gain. More information about Florida Poly's academic integrity policies and procedures can be found here: https://floridapoly.edu/wp-content/uploads/2017/07/FPU-5.005-Academic-Integrity-7.29.14.pdf#search=academic%20integrity

Recording Lectures

Students may, without prior notice, record video or audio of a class lecture for a class in which the student is enrolled for their own personal educational use.

Recordings may not be used as a substitute for class participation or class attendance. Recordings may not be published or shared in any way, either intentionally or accidentally, without the written consent of the faculty member. Failure to adhere to these requirements is a violation of state law (subject to civil penalty) and the student code of conduct (subject to disciplinary action).

Recording class activities other than class lectures, including but not limited to lab sessions, student presentations (whether individually or part of a group), class discussion (except when incidental to and incorporated within a class lecture), and invited guest speakers ***is prohibited***.