NORTHERN ARIZONA UNIVERSITY

School of Informatics, Computing, and Cyber Systems

CYB402 **Applied Cryptography** Syllabus

Term	Class No.	Section	Units	Days & Times	Room	Mode
XXX	XXXX	001	3	N/A	N/A	Online

Enrollment Requirements

Pre-requisites: (CYB136, CS205, MAT226, and (STA 270 or STA 275)) with grades of C or better.

Course Website

http://bblearn.nau.edu

Instructor(s)

Dieter Otte
Email: Dieter.Otte@nau.edu
Office Hours: TBD

Course Description

A practice-oriented approach to crypotography with topics in encryption, randomness, cryptographic security, block ciphers, stream ciphers, hash functions, keyed hashing, authentication, computational complexity, RSA, elliptic curve cryptography, TLS, and post-quantum cryptography.

Course Purpose

This course provides an overview of common cryptography algorithms and related topics. Cryptographic fundamentals are covered (e.g., basic cyphers, random numbers) before surveying common cryptographic algorithms and approaches. More advanced topics in computational complexity are explored before introducing contemporary algorithms such as RSA, elliptic curve cryptography, and TLS. Finally the implications of Quantum Computing are discussed before post-quantum cryptographic algorithms are explored. This course prepares students to understand how cryptographic algorithms work, make approach selections and configurations of those algorithms in industry practice, and appropriately deploy these algorithms in secure applications. Hands-on programming exercises are used to reinforce lectures and provide practical implementation experience. This is a required course in the Bachelor of Science in Cybersecurity program, which builds on mathematical principles from MAT226 (Discrete) and the need for cryptographic algorithms as discussed in previous course work including CYB 136 and CS 205. This course prepares students for coursework that requires a strong understanding of cryptographic principles. This class also directly supports several program student outcomes through its subject matter, student learning, activities, and assessment (student outcomes 1, 2, and 6). This course may be co-convened with CYB502; the graduate course offers significantly more depth with extended homework, a semester long research project, a research paper, and additional reading in cryptographic research.

Course Student Learning Outcomes

Upon successful completion of this course, students will be able to demonstrate the following competencies:

LO1. Describe and explain foundational concepts in cryptography **(evaluation)**;

LO2. Compare and contrast different cryptographic algorithms and their contexts **(analysis)**;

LO3. Appropriately use cryptographic algorithms in a veriaty of contexts **(application)**; and

LO4. Discuss the implications of quantum computing in the context of complexity classes and cryptography **(comprehension)**.

Program Student Outcomes supported by this class

This course directly supports the following program student outcomes in the CYB program assessment and improvement plan:

SO1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

SO2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.

SO6. Apply security principles and practices to maintain operations in the presence of risks and threats.

Assignments / Assessments of Course Student Learning Outcomes

Learning outcomes are assessed through a variety of means:

- Quizzes and exams will assess student ability to describe and explain foundational concepts in cryptography (LO1).
- Homework will be used to assess student ability to compare, contrast, and analyze cryptographic algorithms (LO2 & LO3). Labs will require students to engage with networking tools and utilities used by software engineers, network scientists, and cybersecurity experts throughout industry. Some labs will also require students to implement basic secure network applications using network protocols and security mechanisms covered in this course.
- Discussions on Piazza will be used to assess student understanding of the implications of quantum computing in the context of complexity classes and cryptography (LO4).
- Exams are used to assess student attainment of LO1-LO4.

Grading System

A weighted sum of assessment components is used to determine your final grade in the course:

- Participation in class discussion and activities: **10%**
- Quizzes (at least 6): **10%**
- Homework (at least 6): **30%**
- Exams (2): **50%**

Grades will be assigned using the weighted sum described above using this scale:
A ≥ 90%, **B** ≥ 80%, **C** ≥ 70%, **D** ≥ 60%, **F** < 60%.

There is no "curve". Each student's grade is based on their own outcomes assessments and not affected by the grades of other students. Extra credit opportunities *may* present themselves throughout the semester and will be announced

during class meetings along with the grade category to which they apply. Mistakes in grading do happen, and students are encouraged to discuss such concerns with the instructor during office hours.

Readings and Materials

We will be using the following texts:

- *Serious Cryptography, most recent edition* by Jeane-Philippe Aumasson

Students will also need access to a computer that is capable of running software tools used in labs. It is the responsibility of the student to ensure they are able to complete labs and to communicate with the instructor early on if there is a concern about being able to do so.

Class Outline and Tentative Schedule

The course topics and a *tentative* schedule serve as an outline for the class:

	Dates	Topics	Reading	Assignment
Week 1	TBD	Encryption	SE ch 1	Qz 1
Week 2	TBD	Randomness	SE ch 2	Hw 1
Week 3	TBD	Cryptographic Security	SE ch 3	Qz 2
Week 4	TBD	Block Cyphers	SE ch 4	Hw 2
Week 5	TBD	Stream Cyphers	SE ch 5	Qz 3
Week 6	TBD	Hash Functions	SE ch 6	Hw 4
Week 7	TBD	Keyed Hashing	SE ch 7	Qz 4
Week 8	TBD	Midterm review and midterm exam		
Week 9	TBD	Authenticated Encryption	SE ch 8	
Week 10	TBD	Computational Complexity	SE ch 9	Hw 5
Week 11	TBD	RSA	SE ch 10	Qz 5
Week 12	TBD	Diffie-Hellman	SE ch 11	Hw 6
Week 13	TBD	Elliptic Curves	SE ch 12	Qz 6
Week 14	TBD	TLS	SE ch 13	Hw 7
Week 15	TBD	Quantum Computing and Post-Quantum Encryption	SE ch 14	Qz 7
Week 16	TBD	Final exam		

Due dates for quizzes and homework are posted on BBLearn. Please check BBLearn frequently for updates.

Course Policies

The following policies will apply to this course:

- Students who have not completed the prerequisite(s) for this course, or who do not participate in the first week of class may be administratively dropped from the course.
- The makeup and late work policies are as follows:
    - Quizzes: No make-ups or late submissions allowed.
    - Homework: No make-ups or late submissions allowed.
    - Exams: Make-up exams will be given only in the case of a documented emergency supported by appropriate documentation **and** with approval from the instructor. Make-up exams may be considerably different than the original exam. Make-up exams must be taken within 3 business days of the original exam. Exams are proctored with the ProctorU system.
- Cheating and plagiarism are strictly prohibited. All academic integrity violations are treated seriously. All work you submit for grading must be your own. You are encouraged to discuss the intellectual aspects of assignments with other class participants. However, each student is responsible for formulating solutions independently and in their own words. Academic integrity violations may result in penalties including, but not limited to, a zero on the assignment, a failing grade in the class, or expulsion from NAU.
- Grades will be entered in BBLearn but your final grade will be calculated in Excel using the grading system described above and then entered in LOUIE. Your final course grade will **not** necessarily appear in BBLearn. Please check LOUIE for your final grade.
- The Academic Success Centers offer free tutoring and academic support to improve your study skills and review course material in a number of engineering and math courses. You can schedule an appointment by visiting nau.edu/asc, calling the Academic Success Center at 928-523-7391 or swinging by Dubois Center room 140.
- Email to the instructor and teaching assistants must be respectful and professional. Specifically, all emails should:
    - Contain a salutation, (for example, "Dear Dr. Otte")
    - Contain a closing, (for example, "Best, Jane Doe")
    - Use complete sentences and correct grammar including correct usage of lowercase and uppercase letters. Composing emails on a mobile device is **not** an excuse for poor writing.
    - The body of your message should also be respectful and explain the full context of the query.
    - The subject should be prefixed with "INF110" so that the message can be easily identified. The subject should also use lower case and upper case correctly.
    - Although email will typically be answered quickly, you should allow up to three (3) business days for a response.
    - If you have a question that would require a long response or you have a lot of questions, please come to office hours or schedule an appointment with the instructor.
- Visiting the instructor(s) during office hours is encouraged! I am happy to talk about the class, careers, research, and topics related (even loosely) to this course.

Appendix A. POLICY STATEMENTS FOR COURSE SYLLABI

ACADEMIC INTEGRITY

NAU expects every student to firmly adhere to a strong ethical code of academic integrity in all their scholarly pursuits. The primary attributes of academic integrity are honesty, trustworthiness, fairness, and responsibility. As a student, you are expected to submit original work while giving proper credit to other people's ideas or contributions. Acting with academic integrity means completing your assignments independently while truthfully acknowledging all sources of information, or collaboration with others when appropriate. When you submit your work, you are implicitly declaring that the work is your own. Academic integrity is expected not only during formal coursework, but in all your relationships or interactions that are connected to the educational enterprise. All forms of academic deceit such as plagiarism, cheating, collusion, falsification or fabrication of results or records, permitting your work to be submitted by another, or inappropriately recycling your own work from one class to another, constitute academic misconduct that may result in serious disciplinary consequences. All students and faculty members are responsible for reporting suspected instances of academic misconduct. All students are encouraged to complete NAU's online academic integrity workshop available in the E-Learning Center and should review the full academic integrity policy available at https://policy.nau.edu/policy/policy.aspx?num=100601.

COURSE TIME COMMITMENT

Pursuant to Arizona Board of Regents guidance (Academic Credit Policy 2-224), for every unit of credit, a student should expect, on average, to do a minimum of three hours of work per week, including but not limited to class time, preparation, homework, and studying.

DISRUPTIVE BEHAVIOR

Membership in NAU's academic community entails a special obligation to maintain class environments that are conductive to learning, whether instruction is taking place in the classroom, a laboratory or clinical setting, during course-related fieldwork, or online. Students have the obligation to engage in the educational process in a manner that does not breach the peace, interfere with normal class activities, or violate the rights of others. Instructors have the authority and responsibility to address disruptive behavior that interferes with student learning, which can include the involuntary withdrawal of a student from a course with a grade of "W". For additional information, see NAU's disruptive behavior policy at https://nau.edu/university-policy-library/disruptive-behavior.

NONDISCRIMINATION AND ANTI-HARASSMENT

NAU prohibits discrimination and harassment based on sex, gender, gender identity, race, color, age, national origin, religion, sexual orientation, disability, or veteran status. Due to potentially unethical consequences, certain consensual amorous or sexual relationships between faculty and students are also prohibited. The Equity and Access Office (EAO) responds to complaints regarding discrimination and harassment that fall under NAU's Safe Working and Learning Environment (SWALE) policy. EAO also assists with religious accommodations. For additional information about SWALE or to file a complaint, contact EAO located in Old Main (building 10), Room 113, PO Box 4083, Flagstaff, AZ 86011, or by phone at 928-523-3312 (TTY: 928-523-1006), fax at 928-523-9977, email at equityandaccess@nau.edu, or via the EAO website at https://nau.edu/equity-and-access.

TITLE IX

Title IX is the primary federal law that prohibits discrimination on the basis of sex or gender in educational programs or activities. Sex discrimination for this purpose includes sexual harassment, sexual assault or relationship violence, and stalking (including cyber-stalking). Title IX requires that universities appoint a "Title IX Coordinator" to monitor the institution's compliance with this important civil rights law. NAU's Title IX Coordinator is Pamela Heinonen, Director of the Equity and Access Office located in Old Main (building 10), Room 113, PO Box 4083, Flagstaff, AZ 86011. The Title IX Coordinator is available to meet with any student to discuss any Title IX issue or concern. You may contact the Title IX Coordinator by phone at 928-523-3312 (TTY: 928-523-1006), by fax at 928-523-9977, or by email at pamela.heinonen@nau.edu. In furtherance of its Title IX obligations, NAU will promptly investigate and equitably resolve all reports of sex or gender-based discrimination, harassment, or sexual misconduct and will eliminate any hostile environment as defined by law. Additional important information about Title IX and related student resources, including how to request immediate help or confidential support following an act of sexual violence, is available at http://nau.edu/equity-and-access/title-ix.

ACCESSIBILITY

Professional disability specialists are available at Disability Resources to facilitate a range of academic support services and accommodations for students with disabilities. If you have a documented disability, you can request assistance by contacting Disability Resources at 928-523-8773 (voice), 928-523-6906 (TTY), 928-523-8747 (fax), or dr@nau.edu (e-mail). Once eligibility has been determined, students register with Disability Resources every semester to activate their approved accommodations. Although a student may request an accommodation at any time, it is best to initiate the application process at least four weeks before a student wishes to receive an accommodation. Students may begin the accommodation process by submitting a self-identification form online at https://nau.edu/disability-resources/student-eligibility-process or by contacting Disability Resources. The Director of Disability Resources, Jamie Axelrod, serves as NAU's Americans with Disabilities Act Coordinator and Section 504 Compliance Officer. He can be reached at jamie.axelrod@nau.edu.

RESPONSIBLE CONDUCT OF RESEARCH

Students who engage in research at NAU must receive appropriate Responsible Conduct of Research (RCR) training. This instruction is designed to help ensure proper awareness and application of well-established professional norms and ethical principles related to the performance of all scientific research activities. More information regarding RCR training is available at https://nau.edu/research/compliance/research-integrity.

SENSITIVE COURSE MATERIALS

University education aims to expand student understanding and awareness. Thus, it necessarily involves engagement with a wide range of information, ideas, and creative representations. In their college studies, students can expect to encounter and to critically appraise materials that may differ from and perhaps challenge familiar understandings, ideas, and beliefs. Students are encouraged to discuss these matters with faculty.

Appendix B. ACADEMIC SUPPORT SERVICES

The Academic Success Centers offer free tutoring and academic support to improve your study skills and review course material in a number of engineering and math courses. You can schedule an appointment by visiting nau.edu/asc, calling the Academic Success Center at 928-523-7391 or swinging by Dubois Center in room 140.

Updated 9/20/2019