NORTHERN ARIZONA UNIVERSITY

New Course
Fall 2018

NORTHERN ARIZONA UNIVERSITY | College of Engineering, Forestry, and Natural Sciences
School of Informatics, Computing, and Cyber Systems

INF 638

General Information

- *Course title*: Cryptography and Public Key Infrastructure
- *Semester*: Fall 2017
- *Credit hours*: 3
- *Meeting time and location*: TBD
- *Instructor*: Bertrand Cambou
    - *Instructor email*: bertrand.cambou@nau.edu
    - *Office location*: Bld 90 – Room 110
    - *Office hours*: TBD

Course Prerequisites

Graduate status.

Academic Catalog Description

Study of methods, techniques, and research areas in cryptography and public key infrastructure to strengthen cybersecurity.

Course Purpose

This project-based course is intended to provide a graduate-level study of using nanotechnology in strengthening hardware applications in cybersecurity, including applications in the Internet of Things and government asset protection, and is particularly appropriate as an elective for students in the MSCS, and PHDINF programs. The main objective of the course is to give a practical introduction of Cryptography, with an emphasis on the deployment of public key infrastructure (PKI), leveraging lectures, in-class discussion, in-class assignments, reading assignments, homework assignments, research project literature review, research project implementation and assessment, and research project paper and presentation. The course will start with a general overview of cryptography, and elements of the number theory. The symmetrical cryptographic methods DES, and AES will be described, together with additional elements of the number theory (Galois fields, and extended Galois fields). Elements of quantum cryptography key distribution will be presented. The course will then cover asymmetrical cryptography, the general description of Diffie-Hellman based public key infrastructure, RSA, and Elliptic Curve Cryptography (ECC) with associated mathematical elements (Euclidian and Extended Euclidian algorithms, Euler-Fermat theorems, fast exponential algorithms, formation of cyclic groups for ECC). The course will conclude with the use of cryptography, public key infrastructure deployment, importance of random numbers, digital signatures, and hash functions with SHA algorithm. By the end of the course, students understand the respective strengths and weaknesses of the various cryptographic methods, are able to engage in research applications of cryptography, and PKI in cybersecurity and apply the principles of cybersecurity in a variety of applications in other research areas of interest in computer science, electrical engineering, and informatics.

Student Learning Outcomes

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

- ➢ Analyze, evaluate, and articulate the general uses of cryptography, and PKI in strengthening cybersecurity;
- ➢ evaluate, select, and apply cryptographic algorithms, and embedded software techniques to the design and development of cybersecurity solutions to a variety of application domains;

- identify, interpret, and critically explain the significance of open research areas and questions in cryptography for the design of secure solutions in cybersecurity.
- The student will also acquire a general understanding of the number theory, and mathematics used in modern cryptography.

Course Structure

This offering of INF 638 will consist of lectures, in-class assignments, homework assignments, scholarly literature reading assignments, and a multi-part development project.

Textbook and Required Materials

Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar, Jan Pelzl. (ISBN: 9783642041013).

Recommended Materials and Readings

Additional readings will be provided from various sources, including:

- *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, Shari L. Pfleeger, and Jonathan Margulies (ISBN: 0134085043)
- *Cryptography Decrypted*, by H. X. Mel and Doris M. Baker (ISBN: 9780201616477)
- *Introduction to Modern Cryptography, Second Edition*, by Jonathan Katz and Yehuda Lindell (ISBN: 1466570261)

Course Outline

For a more detailed outline, check the course schedule. Topics will include: introduction to cybersecurity research areas; specific cryptographic methods: symmetrical cryptography, quantum cryptography key distribution, asymmetrical cryptography, PKI and key distribution, need to use true random number generators (TRNG), digital signatures, and hash functions. Elements of mathematics in support of these methods will include the basic number theory, Galois fields, Euclidian algorithms, Euler-Fermat theorems, elliptic curves, and formation of cyclic groups. Breaches in cybersecurity are often due to solutions build on silos, the understanding of the connected disciplines is essentials. This class encourage inter-discipline partnership, and team work. The agenda covered during the semester should be similar than the following (the weekly schedules are approximative, and subject to minor changes):

1- Motivation & Definitions	(week 1)
2- Elements of Number theory	(week 1 to 2)
3- Early Cryptographic methods	(week 2 to 3)
4- Symmetrical Cryptography: DES	(week 3)
5- Symmetrical Cryptography: AES	(week 4 to 5)
6- Quantum Cryptography: Key distribution	(week 5 to 6)
7- Elements of Asymmetrical Cryptography	(week 7 to 8)
8- Asymmetrical Cryptography: RSA	(week 9)
9- ECC Key Distribution	(week 10 to 11)
10- PKI & Digital Signatures	(week 12 to 13)
11- Hash Functions	(week 14)
12- Smartcards	(week 15)

Assessment of Student Learning Outcomes

Methods of assessment include: In-class and reading assignments assess expertise in articulating and evaluating the usefulness of various modern cryptographic methods to protect cyber physical systems under several possible threats; the students need to demonstrate their ability to master elements of the of number theory, and apply it to hide (crypto) the electronic transfer of written texts (-graphy), homework assignments assess student ability to apply cryptographic and embedded software techniques; and a multi-stage research project assesses the ability to identify, interpret, and explain open research questions in cryptography as well as the ability to design and apply solutions to developing secure systems.

Grading System

The weight of each course component toward your final grade is:

Assignment	**Grade Weight %**
Attendance (no miss: 100% - 12 hours miss or more: 0%)	15%
In class assignments (Very active: 100% - passive: 0%)	15%
Homework assignments (To be presented within two working weeks)	15%
Research project #1: Demonstrate understanding of the basic concepts	15%

Research project #2: Demonstrate understanding of the advanced concepts	15%
Research project #3: Demonstrate ability to implement and generalize	15%
Research projects: additional final report	10%

Homework:
The students will have the opportunity to prepare 1-2 homework by session of 2&1/2 hrs. The objectives of the homework are to summarize, and practice elements directly related to the class. This could be some mathematical computations, detailing examples presented in class, or finding additional examples similar than the ones presented. The students are not required to prepare all suggested homework, quality is preferred to quantity. A good student should try to prepare at least 75% of the proposed homework.

Projects:
A project assesses the student ability to select, describe, synthesize and present material related to what is presented in class on a topic of their choice. Examples of successful projects include the programing a small example of ECC key exchange, or the development of a blockchain with SHA-2. The students will be encouraged to present their projects in class, and to prepare small tutorials explaining the context, and bigger picture, of their projects. If they cannot present all three projects in class, the students will have the opportunity to do so during office hours. One of the project can also be a written document submitted at least 5 days before the end of the semester. On demand, and when relevant, the students will have access to the cybersecurity lab to work on their projects. The students will have the latitude to pick a project in line with their general area of expertise, and to partner with one to three peers. If the students wish to present group projects, they need to have different partners for each project. The outcome could be a combination some programming work, and literature work demonstrating their understanding (project#1 &2), and mastering of the subject (project#3).

Grades will be awarded on the following scale:

Percentage Grade	Letter Grade
90% or above	A
80% through 89%	B
70% through 79%	C
60% through 69%	D
59% or below	F

There is no "curve;" your grade is completely up to you and is not affected by the grades of your classmates. Extra credit opportunities may present themselves throughout the semester and be announced during class meetings. If you feel a mistake has been made in grading your assignment, please address your concerns during office hours.

NORTHERN ARIZONA UNIVERSITY
POLICY STATEMENTS FOR COURSE SYLLABI
HTTP://NAU.EDU/CURRICULUM-AND-ASSESSMENT/_FORMS/CURRICULAR-POLICY/SYLLABUS_POLICY_STATEMENTS/

Appendix A. UNIVERSITY POLICY STATEMENTS

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.