INF 638

General Information

- *Course title*: Cryptography and Public Key Infrastructure
- *Semester/Section*: XXXX
- *Credit hours*: 3
- *Meeting time and location*: XXXX
- *Instructor*: XXXX
  - *Instructor email*: XXXX
  - *Office location*: XXX
  - *Office hours*: XXX

Course Prerequisites

Relevant Undergraduate Classes: EE – CS – CE – Applied Mathematics – Applied Physics

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/undergraduate-level study of using cryptography in strengthening 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 final year of a bachelor degree in cybersecurity program in VICEROY. 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 reviews, research project implementation and assessment, and research project papers and presentations. The objective of the course is to provide enough background in mathematics, number theory, and algebra, to be able to understand the main algorithms of mainstream cryptography; however, the priority will be the understanding of the use of cryptography to secure cyber physical systems, and the effective deployment of the Public Key Infrastructure (PKI). The students will therefore be exposed to PKI applications such as digital signatures, blockchains, secure mail, and smartcards for banking and telecommunication applications. By the end of the course, students will understand the respective strengths and weaknesses of the various cryptographic methods, be 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, informatics, and applied mathematics. Breaches in cybersecurity are often due to solutions build on silos, the understanding of these connected disciplines is essentials. This class encourages inter-discipline partnership, and teamwork.

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, apply cryptographic algorithms, and embedded software techniques to the design and development of cybersecurity solutions to a variety of application domains; and
- 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.

Recommended Materials and Readings

Additional readings will be provided from various sources, including:

- *"Understanding Cryptography": A Textbook for Students and Practitioners* by Christof Paar, Jan Pelzl. (ISBN: 9783642041013).
- *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. The course will start with a general overview of cryptography, and the definition of commonly used terms and acronyms used in the field. The course will present elements of the number theory that are important for cryptography such as: modulo arithmetic, inverses, primes and composite numbers, Pascal triangle, and the Chinese Remainder Theorem (CRT). An introduction to early cryptographic methods will be presented: stream ciphers, Caesar, Vigenere, one-time XOR, Random Number Generators; block ciphers, the Data Encryption Systems (DES) with its Feistel scheme. The Advanced Encryption Systems (AES) symmetrical cryptographic method will be described, together with additional elements of the number theory and algebra: Galois finite fields, and extended Galois fields with polynomial arithmetic. The course will then present an overview of asymmetrical cryptography, the description of Diffie-Hellman based public key infrastructure, and the blockchain technology for applications such as cryptocurrencies. The course will review in detail RSA, and Elliptic Curve Cryptography (ECC) with associated mathematical elements: Euclidian and Extended Euclidian algorithms, Euler-Fermat theorems, fast exponential algorithms, monic polynomials, formation of cyclic groups for ECC. The course will conclude with the description of hash functions such as the Standard Hash Algorithm (SHA), and the detailed presentation of digital signatures with hash functions: RSA, Diffie Hellman ECC, El Gamal, NIST, Schnorr.

The agenda covered during the semester should be similar than the following:

1- Motivation & Definitions (week 1)
2- Elements of Number theory (week 2)
3- Early Cryptographic methods (week 3)
4- Symmetrical Cryptography: DES (week 4)
5- Finite fields for cryptography (week 5)
6- Symmetrical Cryptography: AES (week 6)
7- Asymmetrical Cryptography and blockchain technology (week 7)
8- Elements of mathematics for asymmetrical cryptography (week 8- 9)
9- Asymmetrical Cryptography: RSA (week 10)
10- Elliptic Curve Cryptography (ECC) (week 11-12)
11- Hash Functions, and Digital Signatures (week 13-14)

Assessment of Student Learning Outcomes

Methods of assessment include: In-class and reading assignments assess expertise in articulating and evaluating the use of nanoelectronics in authentication; homework assignments assess student ability to apply nanotechnologies to the design of systems; 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 using hardware devices to develop secure systems.

Grading System

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

Assignment	**Grade Weight %**
Homework assignments (To be presented within two working weeks)	20%
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	30%
Research projects: additional final report	20%

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.

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/