INFO 7300/CSYE 7374-02
Engineering Secure Software Systems/Cryptography

Course Information
Course Title: *Engineering Secure Software Systems* or *Cryptography*
Course Number: INFO 7300 or CSYE7374
Term and Year: Fall 2022
Credit Hour: 4
Course Format: Hybrid

Instructor Information
Full Name: Robin Hillyard
Email Address: r.hillyard@northeastern.edu

Course Prerequisites
INFO 6205 Program Structure and Algorithms

Course Description
This course will present an introduction to the software techniques and standards that are used to protect systems and information from various types of attack and exploit. We begin with the mathematical foundation of modern cryptography, including public key encryption and key exchange. This will be followed by a study of practical cyber-security standards, techniques and libraries for information/data scientists to protect applications and data (see Background below).

Along the way, and as time permits, we will touch on related topics such as anonymization, block-chain, Fully Homeomorphic Encryption (FHE), Garbling, and Quantum Computing.

The course will be "hands-on" and involve many assignments as well as a major project. The material is agnostic regarding implementation languages, but Scala will typically be used for examples (no prior experience of Scala is required). Students may use a language of their choice for assignments.

Standard Learning Outcomes

Learning outcomes common to all College of Engineering Graduate programs:

1. *An ability to identify, formulate, and solve complex engineering problems.*
2. *An ability to explain and apply engineering design principles, as appropriate to the program's educational objectives.*
3. *An ability to produce solutions that meet specified end-user needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.*

The Information Systems Program accepts students of different engineering backgrounds with minimum programming skills and produces first class Information Systems engineers that operate at the intersection of real-world complexity, software development, and IT management. Graduating students will be able to construct end-to-end advanced software applications that meet business needs.

Specific Learning Outcomes for the Information Systems program:

1. *Create a strong technical foundation through diverse, high-level courses*

2. *Built crucial interpersonal skills needed to succeed in any industry*
3. *Foster a deep level of applied learning through project-based case studies*

Course Outcomes:

1. Develop an approach to protecting applications.
2. Know and utilize appropriate strategies to keep information private and/or signed.
3. Understand the limitations and vulnerabilities of cryptographic techniques.

Required Materials:

- *To-be-determined*

What is this class all about?

- It's about one of the most important, but fun, aspects of information technology.
- We will take a practical approach, that's to say we will treat the subject matter with an "engineering" mindset.
- We will get a little mathematical where it's appropriate because the foundation of everything we cover is, essentially, mathematics.
- "Knowledge is power" but secret knowledge is much more powerful than general knowledge.

Background

Privacy and cyber security are the pressing issues of the day. In 2019, Northeastern University joined with five other institutions in a joint task force to study the issues (CyberSecurity announcement).

Data breaches of sensitive information and ransomware attacks dominate the news. Accusations of hacking, tampering, and fraud were major stories for both the 2016 and 2020 Presidential elections in the U.S. The stakes are getting higher, and there is no time to lose. It would not be stretching the truth too much to say that World War III has already begun and is a cyber-war rather than a traditional war. A foreign adversary's ability to knock out key infrastructure, such as the power grid, of a country has already been demonstrated and it may be only a question of time before it is used in earnest as a first strike.

On a more personal front, people expect their government to protect their private information. Yet, this problem is not something that can easily be handled by a government. It is a *global* problem. However, the E.U. and the U.S. have legislated for the protection of private health information (HIPAA in the US). Curiously, while many people advocate stronger privacy laws, they are willing to share all kinds of personal information on social media!

In fact, as we will see, the weak link in nearly every case of a cyber attack is a human. There is general agreement in the IT industry that the best way to prevent attacks is to engineer information systems in such a way that systems *protect themselves* from external attacks by negating the actions of careless or nefarious humans. Thus, our engineering students can help protect information systems by learning how to secure applications themselves as well as securing data in rest or in transit. Whether your focus is on data, application development, or QA testing, this class will help you acquire the skills to contribute to the most critical issues in IT organizations world-wide.

The course takes a unique approach to the development of software applications that are secure and in tune with privacy requirements such as HIPAA. You will learn how to perform security analysis and what are the most important assets to protect; how to build secure architectures of applications; how to do to security testing and ensure that the applications fulfill the security requirements in compliance with

rules and regulations. You will learn cryptographic techniques with a focus on encryption, key exchange protocols and management, digital signatures, and certificates.

The final creative, independent project (meant to be an enjoyable and gratifying culmination of the semester) will be to put all of this learning together to build a secure mobile platform of your own for the delivery of sensitive data to devices that cannot be trusted over public networks.

Being limited in size, this course will give you a chance to work closely and thoroughly with the professor as well as with other students engaged in the topic; it will provide in-depth knowledge of the subject. Students (both local and international) who took this class in the past landed lucrative jobs and moved to important positions in the security/privacy areas of the businesses that hired them.

Topics (by no means will all these be covered)

- Introduction to cryptography
    - The role of modular arithmetic and prime numbers
    - Symmetric shared key encryption
    - Asymmetric key encryption
    - Key exchange mechanisms
    - Cryptography libraries
    - Establishing trust in systems and data
    - Digital signatures
    - Blockchain
- Key Management and its challenges
- Understanding Security objectives
    - Integrity, confidentiality, and availability
- Application Security and its challenges
    - Attack patterns
    - How applications fail and become suspectable to attacks
    - OWasp.org Top ten vulnerabilities
    - Securing web applications
        - Front-end, middle, and backend
- Data protection
    - HIPAA
    - Fully Homomorphic Encryption (FHE)
    - Pseudo-homomorphic encryption and anonymization
    - Garbling, and Quantum Computing
- Web frameworks and underlying interaction protocols
    - What could go wrong
    - Controls and protection
    - Weaknesses at front, middle, and backend layers
- Risk and Attack Models
    - Risk Definition: assets, vulnerabilities, impact, and controls
    - Security as a quality problem
    - Assets, vulnerabilities, and attack patterns

    - OWASP Models
- Principles of trust computing
    - Strong Identity Management
        - To determine Authenticity of Signer/User
        - Minimizing the risk of dealing with persons who attempt to escape responsibility by claiming to have been impersonated
    - Accountability and Non-repudiation
        - To provide assurance that the integrity of the data or message has not been compromised or altered
        - Minimizing the risk of undetected data/document tampering and forgery, and of false claims that a document was altered after it was sent
    - Audit support
        - To identify and verify parties' responsibility/liability regarding legally enforceable contracts
- Putting it together: Building end to end secure applications
    - The Kerberos communication protocol for modeling end-to-end secure interactions
- Security Testing Plan
    - Methods and tools
    - Penn testing
    - Coding best practices
    - Code review

Module 1: Cryptography: History and Fundamentals [THIS NEEDS SIGNIFICANT REVISION]

Module Overview

Historical and current encryption methods:
• Caesar cipher, Vigenère cipher, one-time-pad, Enigma machine.
• Search problems, decision problems and inverse operators:
  ○ factorization;
• Prime numbers and their properties as they relate to cryptography.
• Key establishment:
  ○ Key exchange mechanisms, in particular Diffie-Hellman-Merkle.
  ○ Public-private keys, in particular RSA algorithm.

Learning Objectives
By the end of this module, you will be able to do the following: • Implement a Vigenère cipher. • Implement the DHM key exchange. • Implement the RSA algorithm. • Understand the high-level differences between symmetric and asymmetric encryption. • Create and register your own public-private key pair.

Reading and Resources	
Required Resources	**Description**
Optional Resources	Description

Module Content and Tasks

Title: 1.1 Substitution Ciphers **Type:** Embedded Slideshow or link to PowerPoint file **Lesson Description**: This lesson gives a historical background to ciphers.
Title: 1.2 Prime Numbers **Type:** Embedded Slideshow or link to PowerPoint file **Lesson Description:** This lesson introduces the role of prime numbers and factorization in cryptography.

Module 2: Practical Cryptography

Module Overview
Practical cryptography techniques and libraries • Symmetric encryption algorithms, including AES-128. • Public-key registries. • PHP • Standard encryption libraries for the JVM (*JCA* and *BouncyCastle*) and Python (*cryptography*). • SSL and secure HTTP circuits (https://...).

Learning Objectives
By the end of this module, you will be able to do the following: • When to use symmetric versus asymmetric encryption. • Create and register a public-key and how to find those of others. • Know the details of the various symmetric ciphers such as AES 128. • Know how to use standard encryption libraries for the JVM (*JCA* and *BouncyCastle*) and Python (*cryptography*). • Understand the mechanisms behind SSL (https://...).

Module 3: Applications of Cryptography and Anonymization: Information Protection

Module Overview
How to protect identifiable data from bad actors and even bad systems: • Anonymization. • Multi-key encryption • Fully-homomorphic encryption • Pseudo-homomorphic encryption How to protect data from mutation: • Digital signatures and Block-chain; How to protect facts from fakery: • Peer-review, digital signatures

Learning Objectives
By the end of this module, you will be able to do the following: • Design a HIPAA-compliant healthcare information system; • Build your own block-chain-based crypto-currency; • Set up a reference site for facts.

Module 4: Team Project

Module Overview
You will form 2 or 3 person teams and build an information-protection system of some sort.

Learning Objectives
You will get experience of teamwork, software development, testing, etc.

End-of-Course Evaluation Surveys

Your feedback regarding your educational experience in this class is very important to the College of Professional Studies. Your comments will make a difference in the future planning and presentation of our curriculum.

At the end of this course, please take the time to complete the evaluation survey at **https://neu.evaluationkit.com**. Your survey responses are **completely anonymous and confidential**. For courses 6 weeks in length or shorter, surveys will be open one week prior to the end of the courses; for courses greater than 6 weeks in length, surveys will be open for two weeks. An email will be sent to your HuskyMail account notifying you when surveys are available.

Academic Integrity

A commitment to the principles of academic integrity is essential to the mission of Northeastern University. The promotion of independent and original scholarship ensures that students derive the most from their educational experience and their pursuit of knowledge. Academic dishonesty violates the most fundamental values of an intellectual community and undermines the achievements of the entire University.

As members of the academic community, students must become familiar with their rights and responsibilities. In each course, they are responsible for knowing the requirements and restrictions regarding research and writing, examinations of whatever kind, collaborative work, the use of study aids, the appropriateness of assistance, and other issues. Students are responsible for learning the conventions of documentation and acknowledgment of sources in their fields. Northeastern University expects students to complete all examinations, tests, papers, creative projects, and assignments of any kind according to the highest ethical standards, as set forth either explicitly or implicitly in this Code or by the direction of instructors.

Go to http://www.northeastern.edu/osccr/academic-integrity-policy/ to access the full academic integrity policy.

Student Accommodations

Northeastern University and the Disability Resource Center (DRC) are committed to providing disability services that enable students who qualify under Section 504 of the Rehabilitation Act and the Americans with Disabilities Act Amendments Act (ADAAA) to participate fully in the activities of the university. To receive accommodations through the DRC, students must provide appropriate documentation that demonstrates a current substantially limiting disability.

For more information, visit http://www.northeastern.edu/drc/getting-started-with-the-drc/.

Library Services

The Northeastern University Library is at the hub of campus intellectual life. Resources include over 900,000 print volumes, 206,500 e-books, and 70,225 electronic journals.

For more information and for Education specific resources, visit http://subjectguides.lib.neu.edu/edresearch.

Diversity and Inclusion

Northeastern University is committed to equal opportunity, affirmative action, diversity and social justice while building a climate of inclusion on and beyond campus. In the classroom, member of the University community work to cultivate an inclusive environment that denounces discrimination through innovation, collaboration and an awareness of global perspectives on social justice.

Please visit http://www.northeastern.edu/oidi/ for complete information on Diversity and Inclusion

TITLE IX

Title IX of the Education Amendments of 1972 protects individuals from sex or gender-based discrimination, including discrimination based on gender-identity, in educational programs and activities that receive federal financial assistance.

Northeastern's Title IX Policy prohibits Prohibited Offenses, which are defined as sexual harassment, sexual assault, relationship or domestic violence, and stalking. The Title IX Policy applies to the entire community, including male, female, transgender students, faculty and staff.

In case of an emergency, please call 911.

Please visit www.northeastern.edu/titleix for a complete list of reporting options and resources both on- and off-campus.