Master Course Description for EE-418 (ABET sheet)

Title: Network Security and Cryptography

Credits: 4

UW Course Catalog Description

Coordinator: Radha Poovendran, Professor, Electrical and Computer Engineering

Goals: To develop an understanding of the fundamental principles of cryptography and its application to network and communication security. This course will serve as an introduction to the fundamental tools in cryptography and the protocols that enable its application to network and communication security. This course is an introduction to the basic theory and practice of cryptographic techniques used in computer security. We will cover topics including encryption (secret-key and public-key), digital signatures, secure authentication, key management, cryptographic hashing, public key infrastructure, and ethics and challenges associated with the use of computer security in vulnerable world.

Learning Objectives: At the end of this course, students will be able to:

1. *Describe* the basic cryptographic primitives, authentication protocols and why they work, what are the common design errors.
2. *Design, implement and analyze* some of basic algorithms to be covered in class using Python (or other languages such as MATLAB, Mathematica).
3. *Design* algorithms using block ciphers and relate it to the modern symmetric key encryption standards.
4. *Design and analyze* Hash functions for checking message integrity under transmission.
5. *Design and* analyze Message Authentication Codes (MAC)
6. *Analyze* the strength of a given crypto system using classical and modern cryptanalysis tools to be presented in class.
7. *Describe and analyze* authenticated session establishment protocols used in Internet Communication
8. *Describe* the ethical issues related to the misuse of computer security.

Textbook: D. Stinson, *Cryptography Theory and Practice*, 4$^{\text{th}}$ edition, Chapman & Hall/CRC, 2019.

Reference Texts:

1. C. Kaufman, R. Perlman, M. Speciner, *Network Security (Private Communication in a Public World),* Prentice Hall, 2002.
2. A. Menezes, P. Van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.

Prerequisites by Topic:

Either EE 241, or CSE 163 (Python); and either MATH 136 or MATH 208 or MATH 308 (Calculus and Matrix Algebra); and either IND E 315, or MATH/STAT 394, or STAT 390 (Probability and Statistics).

Topics:

1. Introduction to classical cryptography and cryptanalysis (Stinson Chapter 1) [2 weeks]
2. Block Ciphers and the Advanced Encryption Standard (Stinson Chapter 3) [1 week]
3. Public key encryption based on RSA and Integer Factorization (Stinson Chapter 5) [1 week]
4. Public key encryption based on El-Gamal and Discrete Logarithm Problem (Stinson Chapter 6) [1 week]
5. Hash Functions for Message Integrity Verification (Stinson Chapter 4) [1.5 week]
6. Digital signatures (RSA, El-Gamal, DSA) (Stinson Chapter 7) [1 week]
7. Key Management Schemes, Authenticated Key Agreement Schemes (Stinson Chapter 10) [2 weeks]
8. Public Key Infrastructure and the PKI Standard [1 week]
9. Technology, Ethical Challenges, IEEE Code of Ethics related to Security Engineering in a vulnerable world [0.5 week]

Course Structure: The class meets for two lectures a week, each consisting of 2 hours. There is (bi-)weekly homework due that includes small computer projects in Python. One team-oriented project is planned in this course with Python. Course includes one midterm and one final exam. In-class activities include daily quizzes.

Computer Resources: The course uses Python for homework exercises and course projects. Students are expected to use their personal laptops, but they may use the ECE department computers if available.

Grading: 35% Homework, 20% midterm, 15% Project, 25% final exam, 5% in-class quiz participation activity.

ABET Student Outcome Coverage: This course addresses the following outcomes:

H = high relevance, M = medium relevance, L = low relevance to course.

(1) *An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.* **(H)** The course uses mathematical tools. Students must identify and design suitable

algorithms. Engineering judgment is developed through the understanding the limitations and advantages of a given cryptographic algorithm or network security protocol. Throughout the course we emphasize the need to use sound design principles instead of relying on mathematics only. Towards this direction, security protocols that were mathematically correct but had design flaws are discussed. Assignments require students to analyze other protocols with weaknesses. The homework involves solving engineering problems identified by the assignments and exemplified by class discussion. The exams and projects challenge the students to identify the issues and formulate their individual solutions. The students develop an implementation for stream cipher-based encryption of speech.

(2) *An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.* **(M)** The project challenges the students to develop, design and implement different cryptographic algorithms. In most cases, this is implemented in Python.

(3) *An ability to communicate effectively with a range of audiences.* **(M)** Students are required to write up their simulations in an engineering format. The ability to communicate effectively in writing is a portion of the grade received on homework and projects. Students are required to give a short presentation on a selected security topic to the class (depending on the instructor).

(4) *An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.* **(H)** The course covers security vulnerabilities in systems and their societal implications, enabling the students to recognize the ethical dilemmas that they may face in their professions. Impact of good network security protocols is emphasized. We discuss the impact of design and implementation of insecure protocols and the way they can be exploited. Focus here will be to show how to design protocols that are resilient to common security threats such as user collusion.

(5) *An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives.* **(H)** The course project is conducted in teams of up to 4 members and constitute 15% of their grade.

(7) *An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.* **(H)** The course emphasizes the need for evolving current secure system designs as new threats emerge and security assumptions are weakened. Further, pointers to security websites and articles are provided in order to enhance personal knowledge in this developing area.

Prepared By: Radha Poovendran

Last revised: 11/24/2021