MORGANSTATEUNIVERSITY
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

EEGR482 Introduction to Cryptography

Spring 2015
Credits: 3
Online
COURSE SYLLABUS

Instructor: Dr. Farzad Moazzami
Office: SEB, RM 334
Telephone No. (443) 885-4204
Email Address: Farzad.Moazzami@morgan.edu
Office Hours:

References

Cryptography and Network Security, Principles and Practices, William Stallings, 6th edition and up
Other reference material as provided via Bb

Catalog Description

This course will provide practical knowledge on a wide range of cryptography mechanisms and will explore their relationship with today's modern communications and networks. It includes the fundamentals of cryptography, classic and modern encryption, decryption, public and private key structures, digital signature and secure hash functions.
Prerequisite: EEGR 317

Course Requirements

This course is an elective course for all engineering undergraduate students, especially those with the computer engineering, communications concentration, or cyber security interest. This course relates heavily to the EEGR410/480/481/483. In conjunction with the other courses, this course will help the student develop a breadth of understanding in security applications. Students are expected to prepare and participate in the lectures. Lectures will selectively cover material in the text and will draw from other reference sources.
Homework assignments will consist of selected problems from the text and/or other sources. As this topic has a large applied element, class projects will be an important element of the learning experience for this topic. These projects will be accomplished using MATLAB and C programming languages. Projects will represent a significant portion of the grade. Quizzes will be announced or unannounced, in class or online. One examination will be given during the course. A comprehensive final project will be assigned in lieu of final exam. Students will need to propose the final project and get the instructor's approval. Week 7 of the course is dedicated for the final project proposals in the class. Depending on the scope of the project, working in a group is possible, given that the tasks of individuals are well defined in the project proposal. The final project will be presented in the last session of the class.

Course Objectives

The course provides the student with the mathematical background and the theory of cryptographic mechanisms and an introduction to their application in networks and communications links. After finishing this course students will be able to
CO1: explain the importance of Cryptography as the workhorse in cyber security.
CO2: identify and compare the classical encryption techniques and exploit their vulnerabilities.
CO3: design and employ block ciphers such as DES, 3DES, AES and measure their strengths based on their key size.
CO4: relate the number theory into key generation for asymmetric cryptography and explain RSA.
CO5: Compare symmetric and symmetric encryption mechanisms and select appropriate method for each application.
CO6: explain the application of encryption in RSA and authentication methods, HASH, MAC, SHA, and digital signatures.
CO7: implement Suite B algorithms, Data at rest security measure, EC and ID based Crypto techniques.

Detailed Schedule

Course Schedule/Session Format			
Content	**Date**	**Reference**	**Topic**
Module 1		Chapter 1	**Introduction (CO1)**
Module 2		Chapter 2	**Classic Encryption Techniques** (**CO1,2)** Describes classical symmetric encryption techniques. It provides a gentle and interesting introduction to cryptography and cryptanalysis and highlights important concepts.
Module 3		Chapter 3	**Block Ciphers and DES (CO3)** Introduces the principles of modern symmetric cryptography, with an emphasis on the most widely used encryption technique, the Data Encryption Standard (DES). The chapter includes a discussion of design considerations and cryptanalysis and introduces the Feistel cipher, which is the basic structure of most modern symmetric encryption schemes.
Module 4		Chapter 6	**Block Cipher Operation(CO3)** Explores additional topics related to symmetric ciphers. The chapter begins by examining multiple encryption and, in particular, triple DES. Next, we look at the concept of block cipher modes of operation, which deal with ways of handling plaintext longer than a single block. Finally, the chapter discusses stream ciphers and describes RC4.
Module 5		Chapters 5,7	**AES, Confidentiality using Symmetric Encryption (CO3)** The most important development in cryptography in recent years is the adoption of a new symmetric cipher standard, AES. Chapter 5 provides a thorough discussion of this cipher. Beyond questions dealing with the actual construction of a symmetric encryption algorithm, a number of design issues relate to the use of symmetric encryption to provide confidentiality. Chapter 7 surveys the most important of these issues. The chapter includes a discussion of end-to-end versus link encryption, techniques for achieving traffic confidentiality, and key distribution techniques. An important related topic, random number generation, is also addressed.
Module 6		Chapter 4	**Finite fields, Number Theory (CO4)** Finite fields have become increasingly important in cryptography. A number of cryptographic algorithms rely heavily on properties of finite fields, notably the Advanced Encryption Standard (AES) and elliptic curve cryptography. This chapter is positioned here so that concepts relevant to AES can be introduced prior to the discussion of AES. Chapter 4 provides the necessary background to the understanding of arithmetic over finite fields of the form GF(2n).
Module 7		Chapter 8	**Number Theory (CO4)** Most public-key schemes are based on number theory. While the reader can take the number theoretic results on faith, it is useful to have a basic grasp of the concepts of number theory. Chapter 8 provides an overview and numerous examples to clarify the concepts.
Module 8		Exam	
Spring Break			

Module 9		Chapters 9 & 10.1	**Public Key Cryptography and RSA, Key Management(CO5)** Chapter 9 introduces public-key cryptography and concentrates on its use to provide confidentiality. This chapter also examines the most widely used public-key cipher, the Rivest-Shamir-Adleman (RSA) algorithm. Chapter 10 revisits the issue of key management in light of the capabilities of symmetric ciphers. The chapter also covers the widely used Diffie-Hellman key exchange technique and looks at a more recent public-key approach based on elliptic curves.
Module 10		Chapters 11, 12.1	**HASH, MAC, SHA(CO6)** Of equal importance to confidentiality as a security measure is authentication. At a minimum, message authentication assures that a message comes from the alleged source. In addition, authentication can include protection against modification, delay, replay, and reordering. Chapter 11 begins with an analysis of the requirements for authentication and then provides a systematic presentation of approaches to authentication. A key element of authentication schemes is the use of an authenticator, usually either a message authentication code (MAC) or a hash function. Design considerations for both of these types of algorithms are examined, and several specific examples are analyzed. Chapter 12 extends the discussion of the preceding chapter to discuss two of the most important cryptographic hash functions (SHA and Whirlpool) and two of the most important MACs (HMAC) and CMAC.
Module 11		Chapter 13	**Digital Signature and Authentication protocols (CO6)** An important type of authentication is the digital signature. Chapter 13 examines the techniques used to construct digital signatures and looks at an important standard, the Digital Signature Standard (DSS). The various authentication techniques based on digital signatures are building blocks in putting together authentication algorithms. The design of such algorithms involves the analysis of subtle attacks that can defeat many apparently secure protocols. This issue is also addressed in Chapter 14.
Module 12		Special Topics	Suite B algorithms, at rest data Security,…**(CO7)**
Module 13		Special Topics	Special topics : Quantum Key Cryptography, ID based cryptography**(CO7)**
Module 14		Final project presentations and discussion	

Format Online

Grading

Homework assignments	**20%**
Midterm Exam	**20%**
Quizzes	**20%**
Discussion board	**20%**
Final Project	**20%**

NOTE: Any material submitted that is substantially copied from other students without citation or from the Internet will receive a zero grade.

Notes: Expectations and Requirements

1. Students are expected to log on to Bb 3 times a week.
2. Students are expected to be actively engaged on the discussion board conversations.
3. Homework and other assignments are due by midnight of the given due date. Late penalty will be deducted for late submission.
4. A programming assignment might be given in lieu of a quiz.
5. Academic misconduct or cheating during an exam will result in an F grade for the course.