Master Syllabus

Administrative Unit: Computer and Mathematical Sciences Department

Course Prefix and Number: CISS 451

Course Title: Introduction to Cryptography and Computer Security

Number of Credit Hours: 3 Lecture Hours: 3 Laboratory Hours: 0

Catalog Description: An introduction to cryptography and computer security. Topics include cryptographic methods, hash functions, key exchange, secure communication, message authentication, digital signatures, network security, system security, modern day security protocols and standards. Prerequisites: MATH 325 and CISS 245.

Prerequisite(s)/Corequisite(s): MATH 325 and CISS 245.

Text(s): Textbook(s) listed is/are not necessarily the textbook(s) used in the course.


Course Objectives:

• To develop a mathematical foundation for the study of cryptography.
• To understand the role of cryptography in communication over an insecure channel.
• To understand the importance and techniques of network security.
• To understand the impact and inner workings of computer viruses.

Measurable Learning Outcomes:

• Describe several classical cryptosystems.
• Program several classical cryptosystems using a high level programming language.
• Describe the DES encryption and decryption algorithms.
• Program the DES encryption and decryption algorithms using a high level programming language.
• Describe AES encryption and decryption algorithms.
• Program the AES encryption and decryption algorithms using a high level programming language.
• Computer binary field operations including addition, multiplication, reduction, and inversion.
• Compute GCD, multiplicative inverse mod n, and raising to powers mod n using efficient basic number-theoretic algorithms.
• Describe the use of public key cryptosystems in the key exchange problem.
• Describe RSA cryptosystem, including a necessary complexity theoretic assumption for its security.
• Describe various techniques for securing a network.
• Describe SSL and its use in web security.
• Describe and contrast between different viruses.
• Describe the use of digital certificates.
• Describe injection attacks using SQL injections in the context of web applications.
• Describe buffer overflow attacks and prevention strategies.

Topical Outline (major areas of coverage):

• Classical Cryptography and Overview
  • Classical cryptosystems and their cryptanalysis
  • Model of secure communication
  • Security services
  • Overview of attacks
  • X.800 Security Architecture for Open System Interconnection (OSI)
  • Societal and ethical issues

• Private Key Cryptography
  • Data Encryption Standard (DES)
  • Advanced Encryption Standard (AES):
    • Variations on DES
    • RC4, RC5

• Public Key Cryptography
  • Introduction to Number Theory: GCD, Euclidean Algorithm, Extended Euclidean Algorithm, Chinese Remainder Theorem, Fermat’s and Euler’s Theorem
  • RSA (Rivest-Shamir-Adelman)
  • ECC (Elliptic Curve Cryptography)
  • Key management: Diffie-Hellman Key Exchange protocol
  • Pseudo-random number generation
  • Hash functions
  • Message Authentication
  • Digital Signatures and authentication protocols

• Network Security
  • Authentication: Kerberos, X.509 Authentication Service
  • Email: PGP, S/MIME
  • IP Security (IPSec)
• Web Security
• System Security
• Intrusion detection
• Password management
• Viruses
• Firewalls
• Secure software development

Recommended maximum class size for this course: 20

Library Resources: Online databases are available at http://www.ccis.edu/offices/library/resources.asp. You may access them from off-campus using your eServices login and password when prompted.

Prepared by: Dr. Yihsiang Liow

Date: September 12, 2005

NOTE: The intention of the master syllabus is to provide an outline of the contents of this course, as specified by the faculty of Columbia College, regardless of who teaches the course, when it is taught or where it is taught. Faculty members teaching this course for Columbia College are expected to facilitate learning pursuant to the course objectives and cover the subjects listed in the topical outline. However, instructors are also encouraged to cover additional topics of interest so long as those topics are relevant to the course’s subject. The master syllabus is, therefore, prescriptive in nature but also allows for a diversity of individual approaches to course material.

Office of Academic Affairs
12/04