COURSE NUMBER/TITLE:  MSCS-380/580 [MATH-380] CRYPTOGRAPHY

CREDITS:  3

COURSE DESCRIPTION:  Classical and modern encryption methods, including both public-key and symmetric-key cryptosystems; elementary number theory; digital signature schemes and hash functions; introduction to (and countermeasures for) number-theoretic and algebraic cryptanalysis; discrete logarithms; applications to information assurance and cyber-security.  Prerequisite for MSCS-380: MATH-370 and CS-145; No prerequisite for the graduate version MSCS-580.

TEXTBOOK:  Introduction to Cryptography with Coding Theory, 2nd Ed., by Trappe (adopted S08)

COURSE OBJECTIVES:
Upon completion of this course, students will be able to:
1. Demonstrate understanding of the mathematical foundations of cryptography.
2. Explain several public-key and symmetric-key cryptosystems.
3. Demonstrate understanding of the interior structure and operation of several cryptosystems.
4. Analyze cryptographic algorithms for security strengths and weaknesses, including reading and comprehending proofs of security.
5. Implement the computations underlying a cryptographic algorithm in a computer program.
6. Analyze digital signature and hash algorithms for resistance against forgeries, including proofs of security.
7. Explain the role of encryption systems and digital signatures to information assurance and computer security, particularly with regards to e-commerce.
8. Demonstrate comprehension of the algebraic and number-theoretic aspects of RSA by computing an RSA public-private key pair, and using those to encrypt, decrypt, sign, and verify.

ADDITIONAL GRADUATE-LEVEL OBJECTIVES:
Upon successful completion of the course, the graduate level student will be able to
9. Independently research, analyze, and comprehend an advanced and relevant topic in cryptography.
10. Effectively communicate and disseminate their research to a professional audience using mathematical notation, style and formatting.

COURSE OUTLINE:
(Optional topics, time-permitting, annotated with an asterisk: *)
I. Pre-modern Cryptography (Objectives 1, 3, 4)
   A. Encryption with Mono-alphabetic Substitution Ciphers
   B. Cryptanalysis of Mono-alphabetic Substitution Ciphers
   C. *The Vigenère Poly-alphabetic Cryptosystem
II. Number theory (Objectives 1, 3, 4, 5)
   A. Finite Fields
   B. Solving Linear Equations in Modular Arithmetic
   C. The Affine Cipher
D. *Quadratic Residues and Solving Quadratic Equations in Modular Arithmetic
E. *Matrices over Finite Fields and the Hill Cipher
F. *Diffie-Hellman Key Exchange
G. The Chinese Remainder Theorem
H. Generators/Primitive Roots
I. *Linear Feedback Shift Registers in Modular Arithmetic

III. Public-key cryptosystems (Objectives 1, 2, 3, 4, 5, 7, 8)
A. Using the RSA Algorithm (named after Rivest, Shamir, and Adleman)
B. Generating Public-Private Key Pairs
C. Primality Testing
D. *Algorithms for Rapid Computation

IV. Cryptanalysis of the RSA Cryptosystem (Objectives 1, 3, 4, 8)
A. Methods based on Leaked Private Data
B. Methods based on Factoring
C. Short Plaintext Methods
D. *Other Methods

V. Digital Signature Schemes (Objectives 2, 3, 4, 5, 6, 7, 8)
A. Purposes and Applications of Digital Signatures
B. Using RSA for Digital Signatures
C. Types of Collisions and Categories of Resistance
D. The Merkle-Damgård Construction
E. The Birthday Paradox and Consequences for Digest Size
F. Hash Functions
G. *Certificate Schemes
H. Public-Key Infrastructure
I. *Multicollisions and Herding

VI. One-Time Pads (Objectives 1, 3, 4, 5, 7)
A. Operation
B. Proof of Security
C. Practical Limitations

VII. Symmetric-Key Cryptosystems (Objectives 2, 3, 4, 7)
A. The Advanced Encryption Standard (AES)
B. At least one additional Symmetric Cipher (selected by instructor)

VIII. *Other Topics (at instructor’s discretion, time permitting)
A. Recent Developments
B. Elliptic Curve Cryptography

IX. Presentations on Current Topics (Graduate Objectives 9, 10)

Note that somewhere around II or III the graduate students will negotiate the topic of their “independent inquiry” with the instructor. They will conduct research by reading sources jointly identified by the instructor and the student. This will continue through VIII. That activity represents Graduate Objective 9.