COURSE NO./TITLE: MATH-380 Cryptography
CREDIT: 3

COURSE DESCRIPTION: Classical, public-key, and symmetric-key cryptosystems. Basic number theory. Digital signature schemes. Applications to information assurance and cyber security. Prerequisite: MATH-370

TEXTBOOK:

COURSE OBJECTIVES: Upon completion of this course, students will be able to:
1. Understand the foundations of cryptography
2. Explain several public-key and symmetric-key cryptosystems
3. Understand the mathematics behind various cryptosystems
4. Analyze cryptographic algorithms for security strengths and weaknesses
5. Implement a cryptographic algorithm
6. Analyze digital signature algorithms
7. Explore the importance and applications of cryptography in today’s society
8. Apply cryptography to information assurance and computer security

COURSE OUTLINE:
I. Overview of cryptography (Objective 1)
   A. Historic background
   B. Cryptographic algorithms
   C. Types of attacks used to break cryptosystems
II. Number theory (Objective 3)
   A. Modular arithmetic
   B. Greatest common divisors
   C. Congruences
   D. Chinese Remainder Theorem
   E. Primitive roots
   F. Finite fields
III. Classical cryptography (Objectives 1, 2, 3, 4)
   A. Substitution ciphers
   B. Polyalphabetic ciphers
   C. Permutation ciphers
IV. Public-key cryptosystems (Objectives 2, 3, 4, 5, 6)
   A. RSA Algorithm (named after Rivest, Shamir, and Adleman)
      i. Security
      ii. Attacks
      iii. Primality testing and factoring
   B. ElGamal cryptosystem
      i. Discrete log problem
      ii. Security
C. Signature schemes
   i. RSA
   ii. ElGamal
   iii. Digital Signature Standard
V. Symmetric-key cryptosystems (Objectives 2, 3, 4, 7)
   A. Data Encryption Standard
      i. Background and development
      ii. Differential cryptanalysis
      iii. Meet-in-the-middle attacks
   B. Advanced Encryption Standard
      i. Basic algorithm
      ii. Decryption
   C. Diffie-Hellman key exchange
VI. Hash functions (Objectives 2, 3, 4)
   A. One-way hash functions and properties
   B. Secure Hash Algorithm
   C. Birthday attacks
VII. New developments and other topics (Objective 7)
VIII. Applications to information assurance and cyber security (Objective 8)