Tennessee Technological University
Mathematics Department

MATH 4060/5060: Topics in Cryptography

I. COURSE DESCRIPTION FROM CATALOG:

Fundamental concepts of cryptography presented with mathematical background (including groups, fields, elements of number theory, probability and statistics). Special attention will be given to the RSA algorithm, Elliptic Curve Cryptography, the ElGamal public key cryptosystem, Diffie-Hellman key exchange and pseudo random number generators. Lec.3. Cr. 3.

II. PREREQUISITE(S):

C or better in MATH 2010 and C or better in either MATH 3400 or CSC 2700.

III. COURSE OBJECTIVE(S):

To provide knowledge of cryptographic algorithms, protocols, and their uses in the protection of information.

IV. STUDENT LEARNING OUTCOMES:

Upon successful completion of the course students will be able to

1. Describe how and understand why various cryptographic algorithms and protocols work.
2. Describe the application of cryptography in some security applications.
3. Evaluate security mechanism based on cryptography.

V. TOPICS TO BE COVERED:

Concept 0: Introduction.

(a) Some history.
(b) Examples illustrating importance of cryptography

Concept 1: Basics of number theory and algebra:

(a) An overview of the theory of groups and fields
(b) Greatest Common Divisor algorithm and its binary version.
(c) Modular arithmetic, prime numbers, unique factorization, Euler phi function, exponentiation algorithms (binary, shortest addition chain)

Concept 2: Basics of Probability and Statistics.

Concept 3: Major Algorithms:

(a) RSA, factorization problem, Fermat's Little Theorem, The Prime Number Theorem (without proof), primality testing algorithms (including Rabin-Miller),

pseudoprimes, Carmichael Numbers
(b) pseudorandom number generators, secure pseudorandom number generators (Blum-Blum-Shub)
(c) Elliptic Curves and Cryptography, ElGamal Public Key Cryptosystem on elliptic curves
(d) AES

Concept 4: Hashing and Signatures:

(a) Hash functions, secure hash functions, SHA256
(b) Digital signature, ECDSA, ElGamal signature scheme

Concept 5: Key Management:

(a) Diffie–Hellman protocol
(b) ECDH

Concept 6: Other topics

(a) Classical cryptoanalysis.
(b) Differential and man-in-the-middle attacks
(c) Identity-based Cryptography
(d) Cryptography in Virtual Private Networks
(e) Quantum Key Cryptography

VI. POSSIBLE TEXTS AND REFERENCES:

An Introduction to Mathematical Cryptography by J. Hoffstein, J. Pipher, and J. H. Silverman. iLearn access required.

VII. ANY TECHNOLOGY THAT MAY BE USED:

VIII. ADDITIONAL INFORMATION:

Graduate credit is earned on the basis of additional work required by the instructor.

IX. STUDENT ACADEMIC MISCONDUCT POLICY:

Maintaining high standards of academic integrity in every class at Tennessee Tech is critical to the reputation of Tennessee Tech, its students, alumni, and the employers of Tennessee Tech graduates. The Student Academic Misconduct Policy describes the definitions of academic misconduct and policies and procedures for addressing Academic Misconduct at Tennessee Tech. This includes the university plagiarism policy and cheating. For details, view the Tennessee Tech's Policy 217 – Student Academic Misconduct at Policy Central.

X. DISABILITY ACCOMMODATION:

Students with a disability requiring academic adjustments and accommodations must contact the Accessible Education Center (AEC). AEC is located in the Roaden University

Center, Room 112; phone 372-6119. For more information see TTU Policy 340 (Services for Students with Disabilities) at Policy Central.