Institute of Applied Mathematics
METU

Course Code	9700706
Course Title	Special Topics on Cryptanalysis of Symmetric Cipher Systems
Course Credit(s)	
Instructor(s)	Dr. Öznur MUT SAĞDIÇOĞLU
Prerequisites	Introduction to Cryptography, at least one of the high level languages C/C++/Phyton
Course Catalog Description	Cryptanalysis of symmetric key algorithms
Course Objectives	At the end of the course, the student will learn: • Differential cryptanalysis of block ciphers and some variants of differential cryptanalysis methods ◦ Applying practical attacks to a cipher designed in the course • Linear cryptanalysis of block ciphers ◦ Applying a practical attack to a cipher designed in the course • Cryptanalysis of stream ciphers. Adversary models for stream ciphers. • Related key cryptanalysis. • Basic probability theory used in attacks.
Course Learning Outcomes	Student, who passed the course satisfactorily will be able to: • have a theoretical and practical understanding of cryptanalysis of symmetric key algorithms, • possess a good knowledge in linear and differential cryptanalysis (and some variants) of block ciphers, • have a good understanding of cryptanalysis of stream ciphers, • learn related key cryptanalysis and see how this attack can be applied algorithms.
Tentative (Weekly) Outline	1. Introduction to security of symmetric key ciphers. 2. Brief introduction to block ciphers and adversary models for them. 3. Differential cryptanalysis and practical application on a cipher by using one of the high level languages C/C++/Python. 4. Basic probability theory. 5. Linear cryptanalysis and practical application on a cipher by using one of the high level languages C/C++/python. 6. Impossible differential cryptanalysis and practical application on a cipher by using one of the high level languages C/C++/python. 7. Truncated differential cryptanalysis and practical application on a cipher by using one of the high level languages C/C++/python. 8. Boomerang and practical application on a cipher by using one of the high level languages C/C++/python. Amplified boomerang and rectangle attacks. 9. Brief introduction to stream ciphers and adversary models for them. 10. Security of some well-known stream ciphers. 11. Related key cryptanalysis.

Institute of Applied Mathematics
METU

Course Textbook(s)	• William Stallings. Cryptography and Network Security
Supplementary Materials and Resources	• Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. • Douglas R. Stinson. Cryptography: Theory and Practice
ASSESSMENT METHODS	Midterm %30 Final %40 Homeworks %30