Ceng 471 - Cryptography

Asst. Prof. Dr. Serap Şahin

Fall Term 2022

Izmir Institute of Technology
Department of Computer Engineering

Tentative Agenda

Week	CENG471 Cryptography (Friday, 09:45-12:30)
1 (07/10)	Course Introduction -
	Introduction to Cryptography: Basic Concepts of Cryptography and an overview
2 (14/10)	Classical Cryptosystems: Shift Ciphers, Affine Ciphers, The Vigenere Ciphers …
3 (21/10)	Symmetrical Cryptosystems: DES
4 (28/10)	Symmetrical Cryptosystems: AES
5 (04/11)	Mode of Operations Number-Theoretic Reference Problems
6 (11/11)	Midterm 1
7 (18/11)	Asymmetrical Cryptosystems
	Public Key Parameters and RSA,Discrete Logarithms – ElGamal, DHKE etc.
8 (25/11)	Hash Functions and Data Integrity, Digital Signatures
9 (02/12)	Elliptic Curve Cryptography
10 (09/12)	Key Distribution and Management, PKI, X.509
11 (16/12)	Midterm 2
12 (23/12)	Modern Cryptosystems
	Homomorphic Cryptosystems Part 1
13 (30/12)	Untrusted environments and secure operations
14 (06/01)	Post Quantum Cryptography
15 (13/01)	Final Exam

Books:

1) Introduction to Modern Cryptography, Mihir Bellare, Phillip Rogaway, 2005.

2) Handbook of Applied Cryptography, A.Menezes, P.van orschot, S.Vanstone, 1996.

3) An Introduction to Mathematical Cryptography, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, 2008.

.

Grades

Assignments:	25%
Midterms :	40%
Final :	35%