ELE690/790 Contemporary Cryptology

Web page: **http://www.ee.hacettepe.edu.tr/∼usezen/ele790/**

Time schedule: Tuesday 09:00 - 11:50, Seminer Salonu
Lecturer: Assoc. Prof. Umut Sezen

Textbook

1. W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson, 7th Ed., 2017.
2. M. Bishop, *Introduction to Computer Security*, Addison-Wesley, 2004.
3. D. Gollmann, *Computer Security*, Wiley, 3rd Ed., 2011.

Course Contents

1. Computer and Network Security Concepts, and Basic Mathematical Background
2. Symmetric Ciphers (Basics and Historical Perspective, DES and AES etc.)
3. Block Cipher Operation, Pseudorandom Number Generation and Stream Ciphers (RC4 etc.)
4. Asymmetric Ciphers (Public-Key Cryptography, RSA, ECC, Diffie-Hellman Key Exchange etc.)
5. Data Integrity Algotihms (Cryptographic Hash, MAC, Digital Signature)
6. Key Management and Distribution (X.509 Certificates), and User Authentication (Kerberos etc.)
7. Network and Internet Security (Cloud Security, TLS, Wireless Security, E-mail Security and IP Security)

Grading

Homework (20%), Midterm Exam (40%) and Final Exam (40%).