CS 470
Introduction to Applied Cryptography
Spring 2016

INSTRUCTOR: Prof. Dr. Ali Aydm Selçuk
Office: EA 428
Telephone: 290-1352
E-mail: selcuk@cs.bilkent.edu.tr
Office hour: Tuesday 9:40-10:30 or by appointment

ASSISTANT: Mustafa Ozan Karsavuran
Office: EA 505
E-mail: ozan.karsavuran@cs.bilkent.edu.tr
Office hour: Monday 13:40-14:30 or by appointment

TEXTBOOK: Network Security: Private Communication in a Public World,

GRADING:
Attendance: 3%¹
Quiz: 15%
HW & Project: 20%²
Midterm: 31%
Final: 31%

SYLLABUS:
• Traditional cryptosystems
• Block ciphers
• Stream ciphers
• Hash functions
• Public key encryption
• Digital signatures
• Threshold cryptography
• Key management
• Authentication systems
• Kerberos
• IPsec
• SSL/TLS
• E-mail security
• Tor anonymity network
• Instant messaging security
• Weak authentication protocols
• Selected topics

¹ An attendance of at least 50% is required to qualify for the final exam.
² For pass/fail decision, the grade without homeworks and project must be sufficient
(40%) as well as the grade with them.