CS 470
Introduction to Applied Cryptography
Spring 2013

INSTRUCTOR: Dr. Ali Aydin 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 Battal
Office: EA 425
E-mail: mustafa.battal@cs.bilkent.edu.tr
Office hour: Wednesday 14:40-15:30 or by appointment


GRADING:
Attendance: 3%
Quiz: 17%
Project: 9%
Homework: 16%\textsuperscript{1}
Midterm: 25%
Final: 30%

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
• Selected topics

\textsuperscript{1}For pass/fail decision, the grade without homeworks and project must be sufficient as well as the grade with them.