CS 519
Cryptography and Network Security
Fall 2012

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

TEXTBOOK: *Network Security: Private Communication in a Public World, 2nd Edition.* C. Kaufman, R. Perlman, and M. Speciner. Prentice-Hall.

SUPPLEMENTARY BOOKS:
• *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition.* B. Schneier. John Wiley & Sons.
• *Cryptography : Theory and Practice.* D. Stinson. CRC Press.
• *Handbook of Applied Cryptography.* A. Menezes, P. van Oorschot and S. Vanstone. CRC Press. (Available at http://www.cacr.math.uwaterloo.ca/hac/)

GRADING:
Project: 15%
Homework: 25%
Midterm: 30%
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