Semester: Fall 2012  Section: 01

Instructor: Hamza Yesilyurt  Email: hamza@fen.bilkent.edu.tr
Office: SA–106  Phone: 1897
Office hours: Wednesday 3:40–4:30pm, or by appointment


Topics: This course is designed as an introduction to public key cryptology. We will review the mathematical background material as needed. Topics include: The discrete logarithm problem, Diffie-Hellman key exchange, the RSA public key cryptosystem, digital signatures and hash functions.

Exams & grading: 1st Midterm (23%).
2nd Midterm (23%).
Final Exam (23%)
Homework and Presentations (23%)
Quizzes (8%)

Course schedule: Monday 15:40–17:30 Room SB Z04
Thursday 13:40–15:30 Room SB Z04

Course Regulations
1) Student who misses a midterm or the final exam with a valid and documented excuse is entitled to take a make-up exam subject to the approval of the instructor. The make-up exam takes place after the final exam, covers the same material as the final exam. Although the make-up exam takes place at the end of the semester, the student is expected to contact the instructor as soon as possible.
2) Similarities between the homework papers which cannot be explained as coincidence will be treated as cheating.