This is a 3-credit course that focuses on security applications and cryptographic protocols. An overview of cryptography will be given in the first couple of weeks.

**Catalogue Data:** Overview of Cryptography, Identification and Authentication, Access Control, Operating System Security, Key Distribution, TCP/IP Security, IPSec, DNSSEC, WWW Security, SSL and TLS, E-mail Security (PGP, S/MIME), PKI and certificate systems, Viruses, Firewalls, Intrusion Detection, E-commerce Security

**Prerequisite:** Students are expected to come with undergrad level computer networks and operating systems background. Moreover, computer-programming expertise is necessary. CS408 or TE404 is prerequisite. However, if you have not taken one of these courses but have a background on Computer Networks, feel free to inquiry with the instructor for any possible prerequisite override.

**Instructor:** Albert Levi  
FENS 1091, x9563, levi at sabanciuniv edu

**Assistants:** Halit Alptekin, Ömer Mert Candan

**Schedule:**  
Lecture: T 16:40 – 17:30 FASS G022 and Th 10:40 – 12:30, FASS G049  
Lab/Recitation: F 14:40 – 16:30, FENS G032 (both sections will meet there) (we will not use this hour all the time; you will be informed when there is recitation/lab through lab website)

**Text book:** Cryptography and Network Security, 7th edition (5th or 6th editions OK), William Stallings

**Reference:** Computer Security, Dieter Gollmann  

**Tentative Outline**
- Introduction (1 week)
- Overview of Cryptography (2-3 weeks)  
  - Symmetric and Asymmetric Cryptography  
  - Key agreement  
  - Hash functions
- Authentication and Key Distribution Protocols (1-2 weeks)
- Kerberos and Password Management (1 week)
- TCP/IP Security and IPSec (2 weeks)
- WWW Security, SSL and TLS (1 week)
- E-mail Security (PGP, S/MIME, Domainkeys) (2 weeks)
- PKI and certificate systems, (1 week)
- Access Control (1 week)
- Firewalls and Intrusion Detection Systems (1-2 weeks)

**Make-up Policy:** No make-up! If you miss something, you miss it whatever the reason is!

**Student responsibilities and loads (tentative)**
- One in-class midterm and one in-class final exam.
- There will be 5 (+/- 1) labs. The labs will be dedicated to some practical aspects of the course including programming. Labs will be graded either as in-lab performance or as a separate homework or as after-lab performance. Aside the lab homework assignments there will 1-2 lecture related homework assignments. Some homework assignments may require programming. This year we will organize Capture the Flag (CtF) contest as part of homework.
- A programming project on a secure networking application. This project will be done in 2 or 3 stages and you will be able to work in groups of at most 3 people.

**Tentative Grading and Timing**
- Midterm Exam 25-30%  
  April 21, 2017, Friday, 14:40-16:30 (lab/recit hour)  
  week 10
- Final Exam 35-40%  
  as scheduled by ÖK/SR
- Homework, Lab, Project, CtF 30-40%  
  deadlines will be determined separately

**Class Website:** [http://people.sabanciuniv.edu/levi/cs432](http://people.sabanciuniv.edu/levi/cs432)

PLAGIARISM WILL NOT BE TOLERATED