MAT 421–Şifreleme Bilimine Giriş (2014-2015 BAHAR DÖNEMİ)
Ders Uygulama Planı

Dersin Web Sayfası: http://zsaygi.etu.edu.tr/math421-1415Bahar/math421.html

Öğretim Üyesinin Adı Soyadı	**Ders Saatleri ve Ders Yerleri**	**Ofis Numarası ve E-Posta Adresi**
Yrd. Doç. Dr. Zülfükar Saygı	Perş 13.30-15.20 (304) Cuma 10.30-12.20 (296)	321-B zsaygi [at] etu.edu.tr

Ders içeriği:
Temel şifreleme sistemleri: genel prensipler, tek alfabeli ve çok alfabeli sistemler, basit analiz yöntemleri. Açık anahtarlı sistemlerin genel özellikleri. Blok ve akan şifre sistemlerinin genel özellikleri. Boole fonksiyonlarının genel yapısı. Sıkıştırma fonksiyonları ve doğrulama kodları.

Ders kitabı:

- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996. http://www.cacr.math.uwaterloo.ca/hac/

Diğer kaynaklar:

- Neal Koblitz, "A Course in Number Theory and Crytography", Graduate Text in Mathematics, Springer Verlag, 1987.
- Douglas Stinson, "Cryptography: Theory and Practice", CRC Press, 2002.
- William Stallings, "Crytography and Network Security: Principles and Practice", 5th Ed. Pearson Education, 2010.
- Johannes Buchmann, "Introduction to Cryptography", Springer-Verlag, New York, 2001.

Dersin amacı:

1. Kriptoloji (şifreleme) hakkında temel bilgiler vermek.
2. Kriptolojinin güncel uygulamalardaki yerini görmek.
3. Bilinen temel kriptografi algoritmalarını görmek.

Başarı Değerlendirme:

1. Ödev : 25
2. Proje : 20
3. Arasınav : 25
4. Genel Sınav : 40
5. Derse Devam : 15 (Bonus; kaçırılan saat başı -1)

NOT:

1. Dersle ilgili tüm duyurular dersin web sayfasında ilan edilecek.
2. Proje/ödev grupları 3 kişiden oluşturulacak.
3. Bütün ödev ve projeler bilgisayar ortamında ve/veya elle yazılı olarak iletilecek.
4. Ödevler web sayfasından duyurulacaktır. Ödevlerin teslim süresi 14 gündür.
    i. Erken teslim edilen tam ödevler teslim tarihine göre gün sayısı ve ödev zorluk katsayısına bağlı olarak (+ puan)
    ii. Geç teslim edilen ödev soruları teslim tarihine göre soru sayısı, gün sayısı ve ödev zorluk katsayısına bağlı olarak (- puan) ekstra puan alacaktır.

Haftalık ders programı:

Hafta	Konular
1	Temel (Klasik) şifreleme sistemleri ve analizleri
2	Blok şifre sistemleri
3	Blok şifre sistemleri
4	Blok şifre sistemleri
5	Akan şifre sistemleri
6	Akan şifre sistemleri
7	Akan şifre sistemleri
8	Açık anahtarlı sistemler
9	Açık anahtarlı sistemler
10	Açık anahtarlı sistemler
11	Dijital İmzalar ve Özet (Hash) Fonksiyonları
12	Uygulamalar