DERS TANITIM ve UYGULAMA BİLGİLERİ

Dersin Adı	Kodu	Yarıyıl	T+U+L (saat/hafta)	Türü (Z / S)	Yerel Kredi	AKTS
Kriptoloji	CE 602	Bahar	03+00+00	Zorunlu	3	7.5

Akademik Birim:	Bilgisayar Mühendisliği Bölümü
Öğrenim Türü:	Örgün Eğitim
Ön Koşullar	Yok
Öğrenim Dili:	İngilizce
Dersin Düzeyi:	Doktora
Dersin Koordinatörü:	Öznur YAŞAR DİNER
Dersin Amacı:	Bu ders kriptografi primitiflerini, tanınmış kriptosistemlerini ve ilgili algoritmaları tanıtmayı amaçlamaktadır.
Dersin İçeriği:	Klasik kriptografi, modern simetrik kriptosistemleri, açık anahtarlı kriptografi, kriptografik protokoller, asallık testi için algoritmalar ve tamsayıları çarpanlara ayırma, rastgele sayı üretimi.
Dersin Öğrenme Çıktıları (ÖÇ):	
Dersin Öğrenme Yöntem ve Teknikleri	Anlatım, Tartışma, Örnek verme, Problem Çözme, Soru-Cevap, Grup Çalışması

HAFTALIK PROGRAM

Hafta	Konular	Ön Hazırlık

Kadir Has Üniversitesi'nde bir dönem 14 haftadır, 15. ve 16. hafta sınav haftalarıdır.

ZORUNLU ve ÖNERİLEN OKUMALAR

Douglass R. Stinson, Cryptography: Theory and Practice, Third Edition, Chapman and Hall/CRC 2005.

DİĞER KAYNAKLAR

Neal Koblitz, A Course in Number Theory and Cryptography, Second Edition, Springer-Verlag 1994.

DEĞERLENDİRME SİSTEMİ

Yarıyıl İçi Çalışmaları	Sayı	Katkı Payı (%)
Total:	**0**	**0**

İŞ YÜKÜ HESAPLAMASI

Etkinlikler	Sayısı	Süresi (saat)	Toplam İş Yükü (saat)
Toplam İş Yükü (saat):			**0**

1 AKTS = 25 saatlik iş yükü

PROGRAM YETERLİLİKLERİ (PY) ve ÖĞRENME ÇIKTILARI (ÖÇ) İLİŞKİSİ

#	PY1	PY2	PY3	PY4	PY5	PY6	PY7	PY8	PY9	PY10	PY11	PY12

Katkı Düzeyi: 1 Düşük, 2 Orta, 3 Yüksek