Ders Bilgi Formu

Ders Adı	Kodu	Yerel Kredi	AKTS	Ders (saat/hafta)	Uygulama (saat/hafta)	Laboratuar (saat/hafta)
Bilgisayar Güvenliği ve Kriptografi	BLM5101	3	7.5	3	0	0

Önkoşullar	Yok

Yarıyıl	Güz, Bahar

Dersin Dili	Türkçe
Dersin Seviyesi	Yüksek Lisans Seviyesi
Ders Kategorisi	Uzmanlık/Alan Dersleri
Dersin Veriliş Şekli	Yüz yüze

Dersi Sunan Akademik Birim	Bilgisayar Mühendisliği Bölümü
Dersin Koordinatörü	Sırma Yavuz
Dersi Veren(ler)	Hamza Osman İlhan, Sırma Yavuz
Asistan(lar)ı	

Dersin Amacı	To present fundamental concepts and techniques of modern cryptography. To present the core techniques of cryptography and how they can be applied to meet various security objectives
Dersin İçeriği	Modern kriptografinin temelleri, Şifreleme sistemlerinin geçmişi, Temel şifreleme algoritmaları, Simetrik anahthar kriptosistemler, Özüt çıkarma algoritmaları, Şifreleme yöntemleri, Açık anahtar kriptosistemler, Sayısal imza, Anahtar dağıtımı, Anahtar kararlaştırma ve sır dağıtımı, Quantum şifreleme
Opsiyonel Program Bileşenleri	Yok

Ders Öğrenim Çıktıları

1	Öğrenciler sağladığı güvenlik düzeyi ve etkenliği açısından kriptografi protokollerini değerlendirebilir.
2	Öğrenciler kullanılması düşünelen kriptografi protokolünün artı ve eksilerini değerlendirebilir.
3	Öğrenciler temel Kriptografik protorokolleri tasarlayıp sınayabilir.
4	Öğrenciler öngörülen çözüm için uygun kriptografi prokolünü ya da güvenlik standardını belirleyip uygular.
5	Öğrenciler kriptoanaliz yöntemleri hakında bilgi sahibidir.

Haftalık Konular ve İlgili Ön Hazırlık Çalışmaları

Hafta	Konular	Ön Hazırlık
1	Açıklama ve Tanımlar	
2	Şifreleme Sistemlerinin Tarihçesi	
3	Bilgi Teorisi Temelleri	
4	Temel Algoritmalar	
5	Simetrik Anahtar Şifreleme Yöntemleri	
6	Özüt Çıkarma Yöntemleri	
7	Blok Şifreleme Yöntemleri	
8	Midterm 1 / Practice or Review	

9	Blok Şifreleme Yöntemleri - II	
10	RSA	
11	Sayısal İmza	
12	Anahtar Dağıtımı	
13	Anahtar Kararlaştırma	
14	Sır Dağıtım Yöntemleri	
15	Final	
16	Final Sınavı	

Değerlendirme Sistemi

Etkinlikler	Sayı	Katkı Payı
Devam/Katılım		
Laboratuar		
Uygulama		
Arazi Çalışması		
Derse Özgü Staj		
Küçük Sınavlar/Stüdyo Kritiği		
Ödev	3	20
Sunum/Jüri		
Projeler	1	20
Seminer/Workshop		
Ara Sınavlar	1	20
Final	1	40
Dönem İçi Çalışmaların Başarı Notuna Katkısı		60
Final Sınavının Başarı Notuna Katkısı		40
TOPLAM		100

AKTS İşyükü Tablosu

Etkinlikler	Sayı	Süresi (Saat)	Toplam İşyükü
Ders Saati	13	3	39
Laboratuar			
Uygulama			
Arazi Çalışması			
Sınıf Dışı Ders Çalışması	13	5	65
Derse Özgü Staj			
Ödev	3	10	30
Küçük Sınavlar/Stüdyo Kritiği			
Projeler	1	30	30
Sunum / Seminer			
Ara Sınavlar (Sınav Süresi + Sınav Hazırlık Süresi)	1	25	25

Final (Sınav Süresi + Sınav Hazırlık Süresi)	1	35	35
		Toplam İşyükü	224
		Toplam İşyükü / 30(s)	7.47
		AKTS Kredisi	7.5

Diğer Notlar	Yok