DERS TANITIM ve UYGULAMA BİLGİLERİ

Dersin Adı	Kodu	Yarıyıl	T+U+L (saat/hafta)	Türü (Z / S)	Yerel Kredi	AKTS
Uygulamalı Kriptoloji	CCIP 524	Bahar	03+00+00	Seçmeli	3	7.5

Akademik Birim:	Siber Güvenlik
Öğrenim Türü:	Örgün Eğitim
Ön Koşullar	Yok
Öğrenim Dili:	İngilizce
Dersin Düzeyi:	Yüksek Lisans
Dersin Koordinatörü:	Mahmut Çavur
Dersin Amacı:	• Klasik ve modern şifreleme ile ilgili temel kavramları ve temellerini güçlü bir şekilde kavramak. • Kriptografik düzeyde güvenliğin nasıl tanımlandığını ve kanıtlandığını anlama. • Genel saldırıları ve bunların nasıl önleneceğini anlama. • Eldeki güvenlik mühendisliği (ve yönetimi) sorununa uygun şifreleme tekniklerini uygulama becerisi kazanma.
Dersin İçeriği:	Dersin ilk kısmı kriptografi ile ilgili kavramları ve teorileri kapsayacaktır. Dersin ikinci kısmı, çeşitli güvenlik alanlarındaki kriptografi uygulamalarına odaklanacak.
Dersin Öğrenme Çıktıları (ÖÇ):	• **1-** Kriptografinin genel güvenlikte oynadığı rolün anlaşılması. • **2-** Çeşitli gerçek dünya senaryoları için en iyi uygulama şifreleme şemalarını kullanma yeteneği. • **3-** Çeşitli şemalarda saldırıların pratik bilgisi. • **4-** Eldeki uygulama için blok ve akış şifreleri için doğru çalışma modunu uygulama yeteneği. • **5-** Tam olarak SSL / TSL, VPN'ler ve diğer gerçek dünya uygulamalarının kriptografi kullandığını bilmek.
Dersin Öğrenme Yöntem ve Teknikleri	Sınıf dersleri, ödevler, vize ve final sınavları, Laboratuar uygulamaları.

HAFTALIK PROGRAM

Hafta	Konular	Ön Hazırlık
1	Şifrelemeye genel bakış. Şifre nedir?	Bölüm 1
2	Tek seferlik pad ve stream şifreleri	Bölüm 2
3	Blok şifreleri	Bölüm 3
4	Blok şifre soyutlamaları: PRP'ler ve PRF'ler	Bölüm 4
5	Blok şifrelere yapılan saldırılar	Bölüm 5
6	Mesaj bütünlüğü: tanım ve uygulamalar	Bölüm 6
7	Çarpmaya dayanıklı karma	Bölüm 7
8	Arasınav	
9	Kimliği doğrulanmış şifreleme: etkin saldırılara karşı güvenlik	Bolüm 8
10	Aritmetik modulo primerleri	Bölüm 9
11	itmetik modulo primerleri kullanarak şifreleme	Bölüm 10
12	Genel anahtar şifreleme	Bölüm 11
13	Aritmetik modulo kompozitler	Bölüm 12
14	Kimlik protokolleri	Bölüm 15

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

ZORUNLU ve ÖNERİLEN OKUMALAR

Introduction to Modern Cryptography (2nd edition) by J. Katz and Y. Lindell.

DİĞER KAYNAKLAR

A Graduate Course in Applied Cryptography (V 0.4) by D. Boneh and V. Shoup.

DEĞERLENDİRME SİSTEMİ

Yarıyıl İçi Çalışmaları	**Sayı**	**Katkı Payı (%)**
Proje	1	10
Ödev	3	15
Ara Sınavlar/Sözlü Sınavlar/Kısa Sınavlar	5	35
Final Sınavı	1	40
Total:	**10**	**100**

İŞ YÜKÜ HESAPLAMASI

Etkinlikler	**Sayısı**	**Süresi (saat)**	**Toplam İş Yükü (saat)**
Ders Saati	14	3	42
Proje	1	20	20
Ödev	3	15	45
Dersle İlgili Sınıf Dışı Etkinlikler	9	3	27
Ara Sınavlar/Sözlü Sınavlar/Kısa Sınavlar	1	40	40
Final Sınavı	1	25	25
Toplam İş Yükü (saat):			**199**

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
OC1				1			2				3	

OC2				1			2				3	
OC3				1			2				3	
OC4				1			2				3	
OC5				1			2				3	

Katkı Düzeyi: 1 Düşük, 2 Orta, 3 Yüksek