Меѓународен Универзитет Визион - International Vision University
Universiteti Ndërkombëtar Vizion - Uluslararası Vizyon Üniversitesi

Adres: Ul. Major C. Filiposki No.1, Gostivar – Makedonya
tel: +389 42 222 325, www.vizyon.edu.mk, info@vizyon.edu.mk

DERS İZLENCESİ (SYLLABUS)

DERSİN ADI	DERSİN KODU	YARIYILI	DERS YÜKÜ	AKTS
KRİPTOGRAFİYE GİRİŞ	**4029**	**5**	**180**	**6**

Ön Şartlı Dersler	Yok

Dersin Dili	Türkçe
Dersin Türü	Seçmeli
Dersin Seviyesi	Lisans
Dersin Öğretim Üyesi	
Dersin Yardımcıları	
Derslik	
Ders Dışı Görüşme Saatleri ve Yeri	**Görüşme** **Danışmanlık:**

Dersin Amacı	Kriptolojiye giriş dersi, ağ güvenliği ve şifreleme teknikleri konularında bir giriş yaparak öğrencinin ağ güvenliği ile ilgili alt yapısını oluşturarak geleneksel ve modern şifrelerinin tasarımları üzerine bilgi verme ve bunların uygulama alanlarının önemini vurgulama hedefindedir. Bu derste simetrik şifreleme yöntemleri ve bu yöntemlere yönelik saldırılar konusunda öğrencinin alt yapısının oluşturulması amaçlanmaktadır.
Dersin Öğrenme Çıktıları	Bu dersin sonunda öğrenciler • Temel şifreleme yöntemlerini öğrenir, • Simetrik şifreleme yapılarını ve bu yapılara karşı olan saldırıları kavrar, • Önemli şifreleme algoritmalarını kavrayarak bu algoritmaların yazılım uygulamalarını programlama dillerinden biriyle (örneğin C ile) gerçekleştirebilir,
Dersin İçeriği	Ders, çeşitli ağ güvenliği alanında güvenlik amaçları üzerine geniş bir giriş yapılarak, aşağıdaki konu başlıkları ile devam etmektedir: Ağ Güvenliğinde güvenlik amaçları. Kriptografinin Matematiği. Geleneksel Simetrik Anahtarlı Şifreler. Cebirsel Yapılar. Modern Simetrik Anahtarlı Şifrelere Giriş. Veri Şifreleme Standardı. Gelişmiş Şifreleme Standardı. Modern Simetrik Anahtarlı Şifrelerle Şifreleme. Akan Şifreleme Yöntemleri. Doğrusal Kriptanaliz. Diferansiyel Kriptanaliz. Kriptografik Özet Fonsiyonları. Kriptografik Özet Fonsiyonları. Simetrik Anahtar Dağıtımı.

HAFTALIK KONULAR VE İLGİLİ ÖN HAZIRLIK ÇALIŞMALARI

Hafta	Konular	Ön Hazırlık
1	Ağ Güvenliğinde güvenlik amaçları.	Ders notunun ve kaynaklarının ilgili kısımları
2	Kriptografinin Matematiği.	Ders notunun ve kaynaklarının ilgili kısımları
3	Geleneksel Simetrik Anahtarlı Şifreler.	Ders notunun ve kaynaklarının ilgili kısımları
4	Cebirsel Yapılar.	Ders notunun ve kaynaklarının ilgili kısımları
5	Modern Simetrik Anahtarlı Şifrelere Giriş.	Ders notunun ve kaynaklarının ilgili kısımları
6	Veri Şifreleme Standardı.	Ders notunun ve kaynaklarının ilgili kısımları
7	Ara Sınav	Ders notu ve kaynakları
8	Gelişmiş Şifreleme Standardı.	Ders notunun ve kaynaklarının ilgili kısımları
9	Modern Simetrik Anahtarlı Şifrelerle Şifreleme.	Ders notunun ve kaynaklarının ilgili kısımları
10	Akan Şifreleme Yöntemleri.	Ders notunun ve kaynaklarının ilgili kısımları
11	Doğrusal Kriptanaliz.	Ders notunun ve kaynaklarının ilgili kısımları
12	Diferansiyel Kriptanaliz.	Ders notunun ve kaynaklarının ilgili kısımları
13	Kriptografik Özet Fonsiyonları.	Ders notunun ve kaynaklarının ilgili kısımları
14	Kriptografik Özet Fonsiyonları.	Ders notunun ve kaynaklarının ilgili kısımları
15	Dönem Sonu Sınavı	Ders notunun ve kaynaklarının tamamı

AKTS VE DERS YÜKÜ TABLOSU

Sunum / Seminer			
Sınıf Dışı Ders Çalışma (ön hazırlık ve pekiştirme)	14	3	42
Ara Sınav	1	12	12
Yarıyıl Sonu Sınavı	1	14	14
Toplam Ders Yükü			
AKTS	**6**		

DERSLE İLGİLİ GENEL İLKELER

Değerli Öğrencilerimiz,

Derse dahil olmanız, dersi tam öğrenmeniz ve hak ettiğiniz başarıyı elde etmeniz amacıyla her derse, işlenecek konularla ilgili bölümleri temel ve yardımcı ders kitaplarından okuyarak hazırlıklı gelmeniz gerekmektedir. Ders saatlerine titizlikle uymanızı, çok zaruri olmadıkça dersleri aksatmamanızı, derse aktif katılım sağlamanızı, hocanızla ve sınıf arkadaşlarınızla tam iletişim kurmanızı, sınıftaki tartışmalara katılarak aktif olmanızı bekliyoruz. Gerek derslerde, gerekse sınavlarda meydana gelebilecek etik-dışı davranışlar konusunda ilgili yönetmelik çerçevesinde hareket edilecektir. Her dersin başında, ortasında veya sonunda olmak üzere hocanızın istediği bir zamanda yoklama alınacaktır. Dönem boyunca bütün derslere katılan öğrenciye, sınav notuna ek olarak 15 puan devam notu verilecektir.

KAYNAKLAR

ANA KAYNAK		
No	**Kitabın İsmi**	**Yazarın İsmi, Yayın Evi, Yayın Yılı**
1	Kriptografi / Şifrelerin Matematiği	Canan Çimen , Sedat Akleylek , Ersan Akyıldız, ODTÜ GELİŞTİRME VAKFI YAYINCILIK VE İLETİŞİM A.Ş. ,2007
2		
3	Cryptography and Network Security	Behrouz A. Forouzan

YARDIMCI KAYNAKLAR		
No	**Kitabın İsmi**	**Yazarın İsmi, Yayın Evi, Yayın Yılı**
1	Kriptoloji Uygulamaları	Hüseyin Bodur
2		
3	Introduction to Cryptography with Coding Theory	Wade Trappe and Lawrence C. Washington

DEĞERLENDİRME SİSTEMİ

Değerlendirmede Esas Alınan Çalışmalar	SAYISI	KATKI PAYI
Devam	15	%10
Proje / Etkinlik	1	%20
Ara Sınav	1	%35
Dönem Sonu Sınavı	1	%35
TOPLAM	**17**	**%100**

ÜNİVERSİTE ETİK KODU

Sınavlarda kopya yapılması veya yapmaya teşebbüs edilmesi, dersle ilgili ödev, proje, sunum gibi çalışmalarda kullanılan kaynaklara atıf yapılmaması (intihal) durumlarında M.C. Eğitim Bakanlığı ve Uluslararası Vizyon Üniversitesinin mevzuatında yer alan ilgili disiplin kuralları uygulanır. Uluslararası Vizyon Üniversitesi öğrencilerinin bu tarz davranışlara asla rağbet etmemeleri beklenmektedir.