DERS BİLGİLERİ					
Ders	*Kodu*	*Yarıyıl*	*T+U+L Saat*	*Kredi*	*AKTS*
Kriptoloji ve Siber Güvenlik	CIS 520		3+0+0	3	10

Ön Koşul Dersleri	-

Dersin Dili	İngilizce
Dersin Seviyesi	Lisans
Dersin Türü	Zorunlu
Dersin Koordinatörü	Dr. Öğr. Üyesi Mustafa Asım Kazancıgil
Dersi Verenler	
Dersin Yardımcıları	
Dersin Amacı	Bu dersin amacı, öğrencilere siber güvenlik alanında kullanılan kriptoloji yöntemleri ve kriptografi türlerini öğretmektir.
Dersin İçeriği	Siber güvenlik alanında kullanılan kriptoloji yöntemleri ve kriptografi türlerinin temelleri, modüler aritmetik, şifreleme protokolleri, vigenere şifreleme ve lineer şifreleme, açık anahtarlı şifreleme algoritması, RSA şifreleme yönetimi, asal sayılar, ikame şifrelemesi, Sezar şifrelemesi, Kerberos DC kriptografisi, tersine çarpım, genişletilmiş Öklid algoritması, karşılaştırma ve fark aramalı kriptografik algoritma

Dersin Öğrenme Çıktıları	**Program Öğrenme Çıktıları**	**Öğretim Yöntemleri**	**Ölçme Yöntemleri**
Bilgi Sistemleri mezunları, işletim sistemlerinin ve ağların temel bileşenlerini bilir.	3,6,9	1,3,4	A,B,C
Bilgi Sistemleri mezunları temel işletim sistemi güvenlik tehditlerinin ne olduğunu bilir.	2,3,6,9	1,2,3,4	A,B,C
Bilgi Sistemleri mezunları, ağlardaki temel güvenlik tehditlerinin ne olduğunu bilir.	3,6,9	1,3,4	A,B,C
Güvenlik protokollerini ve uygulanmasını bilir.	2,6,9	1,3,4	A,B,C
Güvenlik tehditlerine ve saldırılara karşı nasıl önlem alınacağını bilir.	3,6,9	1,3,4	A,B,C,D
Şifreleme önlemlerini bilir ve uygular.	3,6,9	1,2,3,4	A,B,C,D
Kimlik doğrulama önlemlerini bilir ve uygular.	3,9	1,2,3,4	A,B,C,D
Etik hacklemeyi bilir.	3,6,9	1,3,4	A,B,C,D

Öğretim Yöntemleri:	
Ölçme ve Değerlendirme Yöntemleri:	

DERS AKIŞI		
Hafta	**Konular**	**Ön Hazırlık**
1	Kriptografi ve Siber Güvenlğin Temelleri	
2	Kriptografi ve Siber Güvenliğin Temelleri	
3	Modüler Aritmetik	
4	Modüler Aritmetik	
5	Kriptografi Protokolleri	
6	Ara Sınav	
7	Vigenere Şifreleme ve Lineer Şifreleme	
8	Açık Anahtarlı Şifreleme Algoritması, RSA Şifreleme Yönetimi	
9	Asal Sayılar, İkame Şifrelemesi ve Sezar Şifrelemesi	
10	Kerberos DC Kriptografisi Tersine Çarpım	
11	Genişletilmiş Öklid Algoritması	
12	Karşılaştırma ve Fark Aramalı Kriptografik Algoritma	
13	Final Sınavı	

KAYNAKLAR	
Ders Notu	Harriet Fell & Javed Aslam (2017): “Discrete Structures”. Cognella Academic Publishing. ISBN-10: 1634876466. ISBN-13: 978-1634876469.
Diğer Kaynaklar	

MATERYAL PAYLAŞIMI	
Dokümanlar	Sunumlar ve Laboratuvar Föyleri
Ödevler	Ödev Föyleri
Sınavlar	Eski Sınav Soruları öğrencilere verilmektedir

DEĞERLENDİRME SİSTEMİ		
YARIYIL İÇİ ÇALIŞMALARI	**SAYI**	**KATKI YÜZDESİ**
Ara Sınav	1	30
Final	1	70
Toplam		**100**
Finalin Başarıya Oranı		70
Yıl içinin Başarıya Oranı		30
Toplam		**100**

DERSİN PROGRAM ÇIKTILARINA KATKISI							
No	Program Öğrenme Çıktıları	Katkı Düzeyi					
		1	2	3	4	5	
1	Bilgi Güvenliği Teknolojisi mezunu, gelişen bilgisayar teknolojileri ile ortaya çıkan çoklu ortamlardaki siber güvenlik tehditleri ve bunları etkisiz hale getirmek için kullanılan kriptoloji yöntemleri konusunda bilgi sahibidir.						
2	Bilgi Güvenliği Teknolojisi mezunu, gelişen bilgisayar teknolojileri ile ortaya çıkan çoklu ortamlarda kullanıcılara amaçlarına uygun bilgisayar uygulamalarının tasarlanması, geliştirilmesi ve kullanılabilmesi için gerekli sistemlerin oluşturulması konusunda ileri bilgi sahibidir.			x			
3	Bilgisayar biliminin temel işleyişini ve problemlerini soyut matematik çerçevesi içinde çözebilmek için gerekli algoritma veri yapılarını tasarlayabilen, geliştirilebilen ve uygulayabilen bilgi ve beceriye sahiptir.					x	
4	Bilişim mezunu, günümüze kadar geliştirilen yapısal yazılım geliştirme araçlarıyla amacına uygun yazılım mantığını tasarlayabilme, bu yazılımları geliştirebilme ve farklı donanım ortamlarında uç kullanıcıların kullanımına sunabilme bilgi ve becerilerine sahiptir.				x		
5	Bilişim mezunu, günümüze kadar geliştirilen nesne yönelimli yazılım geliştirme araçlarıyla amacına uygun yazılım mantığını tasarlayabilme, bu yazılımları geliştirebilme ve farklı donanım ortamlarında uç kullanıcıların kullanımına sunabilme bilgi ve becerilerine sahiptir.	x					
6	Bilişim mezunu, bilgisayarların temel bileşeni işletim sistemlerinin işleyiş mantığını, sistemde işlerin ve kullanıcı yetkilerinin yönetimi için komutların geliştirilmesi ve farklı donanımsal ortamlarda uygulanmasını bilir. Veri akışının güvenli bir biçimde yapılabilmesi için gereken kriptoloji metodları ve tekniklerine hakimdir.					x	
7	Bilişim mezunu, veri kavramı, yapıları, modelleri ile veritabanı uygulamalarını kullanma ve ilişkisel veri tabanlarında veriyi erişim ve işleme araçlarını tasarlama, geliştirme ve uygulama hakkında bilgi ve becerilere sahiptir.		x				
8	Bilişim mezunu, ticari amaçlı yazılımların veri depolarının modellenmesi, yazılımdan bağlanarak veriye erişimin güvenli bir biçimde yapılabilmesi ve verilerin işlenmesi konularında ilgili yazılım araçlarıyla geliştirme ve uygulayabilme bilgi ve becerilerine sahiptir.						
9	Bilişim mezunu, bilgisayar ağlarının temellerini, ağ sistemin tasarlanması ve yapılandırılması, güvenliği, bakımı ve sorunlarını çözebilmek için gerekli ve yeterli bilgi birikimine sahiptir.					x	
10	Bilişim mezunu, günümüzün en büyük bilgisayar ağı olan internete özel olarak görsel ara yüzlerin ve çoklu katmanlı istemci/sunucu mimarisinde çalışabilecek yazılımların tasarlanması, geliştirilmesi ve uygulanabilmesi için gerekli bilgi, beceri ve donanıma sahiptir.					x	

AKTS / İŞ YÜKÜ TABLOSU			
Etkinlik	SAYISI	Süresi (Saat)	Toplam İş Yükü (Saat)
Ders Süresi (Sınavlar dahildir: 13x toplam ders saati)	13	3	39
Sınıf Dışı Ders Çalışma Süresi (ön çalışma, pekiştirme)	14	4	56
Ara Sınav	1	2	2
Ödev	4	35	140
Final	1	3	3
Toplam İş Yükü			240
Toplam İş Yükü / 25 (s)			9.60
Dersin AKTS Kredisi			10