

GENEL TANIM / GENERAL DESCRIPTION

Ders Adı / Course Name	Computer Engineering and Cryptography / Computer Engineering and Cryptography	
Ders Kodu / Course Code	BLG504	
Ders Türü / Course Type		
Ders Seviyesi / Course Level	Master with Thesis / Master with Thesis	
Ders Akts Kredi / ECTS	6.00	
Haftalık Ders Saati (Kuramsal) / Course Hours For Week (Theoretical)	0.00	
Haftalık Uygulama Saati / Course Hours For Week (Objected)	0.00	
Haftalık Laboratuar Saati / Course Hours For Week (Laboratory)	0.00	
Dersin Verildiği Yıl / Year	1	
Öğretim Sistemi / Teaching System	Daytime Class / Daytime Class	
Eğitim Dili / Education Language		
Ön Koşulu Olan Ders(ler) / Precondition Courses	Yok	None
Amacı / Purpose	Bu ders, modern kriptografinin temelleri, şifreleme sistemlerinin geçmişi ve temel şifreleme algoritmaları gibi konuları kapsamaktadır. Ayrıca, simetrik anahtar kriptosistemleri, özüt çıkarma algoritmaları, şifreleme yöntemleri ve açık anahtar kriptosistemleri gibi konuları da ele almaktadır. Ders aynı zamanda sayısal imza, anahtar dağıtımı, anahtar kararlaştırma ve sır dağıtımı gibi önemli konuları da kapsamaktadır. Öğrenciler, bu ders sayesinde güvenli iletişim ve veri koruma konularında temel bilgileri öğrenirken, kriptografi alanındaki temel prensipleri ve uygulamaları anlama fırsatı bulacaklardır. Son olarak, ders kuantum şifreleme konusuna da değinmektedir. Öğrenciler, kuantum şifreleme alanındaki temel kavramları ve yöntemleri öğrenerek, gelecekteki güvenlik ihtiyaçlarına yönelik yeni yaklaşımlar hakkında bilgi sahibi olacaklardır. Bu ders, öğrencilere kriptografi konusunda sağlam bir temel sunmak ve güvenliğin önemini vurgulamak amacıyla tasarlanmıştır. Öğrenciler, ders süresince teorik konuları öğrenirken, pratik uygulamalar ve gerçek dünya senaryoları üzerinde çalışarak kriptografi becerilerini geliştirme fırsatı bulacaklardır	
İçeriği / Content	"Bilgisayar Güvenliği ve Kriptografi" dersi, bilgisayar sistemlerinin güvenliğini sağlamak için temel prensipleri ve teknikleri inceler. Öğrenciler, bilgisayar korsanlığı tehditleri, şifreleme teknikleri, ağ güvenliği, güvenlik politikaları ve savunma stratejileri gibi konuları öğrenirler. Ders, öğrencilere bilgi teknolojileri alanında güvenlik uzmanları olarak kariyer yapmak için gerekli olan temel bilgi ve becerileri sağlar. Bu ders, bilgi güvenliği konusunda güçlü bir temel oluşturarak, öğrencilerin dijital dünyadaki güvenlik zorluklarıyla başa çıkmasına yardımcı olur. "The Computer Security and Cryptography" course explores the fundamental principles and techniques to secure computer systems. Students learn about computer hacking threats, encryption techniques, network security, security policies, and defense strategies. The course provides students with the essential knowledge and skills needed to pursue careers as security experts in the field of information technology. By establishing a strong foundation in information security, this course helps students tackle security challenges in the digital world effectively.	

Önerilen Diğer Hususlar / Recommended Other Considerations	Yok	None
Staj Durumu / Internship Status	Yok	None
Kitabı / Malzemesi / Önerilen Kaynaklar / Books / Materials / Recommended Reading	Antoine Joux, Algorithmic Cryptanalysis, CRC Press, 2009	Antoine Joux, Algorithmic Cryptanalysis, CRC Press, 2009
Öğretim Üyesi (Üyeleri) / Faculty Member (Members)		

ÖĞRENME ÇIKTILARI / LEARNING OUTCOMES

1	Öğrenciler, bilgisayar sistemlerini etkileyebilecek çeşitli güvenlik tehditlerini tanıyacak ve analiz edeceklerdir.	Students will recognize and analyze various security threats that can affect computer systems.
2	Öğrenciler, şifreleme teknikleri ve algoritmalarını anlayarak, verilerin güvenliğini sağlamak için kriptografiyi etkili bir şekilde uygulayabileceklerdir.	By understanding encryption techniques and algorithms, students will effectively apply cryptography to ensure data security.
3	Öğrenciler, güvenli ağlar oluşturmak ve ağ tabanlı saldırılara karşı korunmak için gerekli stratejileri geliştireceklerdir.	Students will learn network security principles to develop necessary strategies for creating secure networks and protecting against network-based attacks.
4	Öğrenciler, kuruluşlar için etkili güvenlik politikaları geliştirmek ve uygulamak için gereken bilgiyi kazanacaklardır.	Students will gain the knowledge required to develop and implement effective security policies for organizations.
5	Öğrenciler, yazılım ve sistemlerdeki güvenlik açıklarını tespit etme yeteneklerini geliştirerek, bu açıkları kapatmak için etkili savunma stratejileri oluşturabileceklerdir.	By enhancing their ability to identify security vulnerabilities in software and systems, students will create effective defense strategies to address these vulnerabilities.

HAFTALIK DERS İÇERİĞİ / DETAILED COURSE OUTLINE

Hafta / Week					
1	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Temel Kavramlar				
	Basic Concepts				
2	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Şifreleme Sistemlerinin Tarihçesi				
	History of Encryption Systems				
3	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Bilgi Teorisi Temelleri				
	Foundations of Information Theory				
4	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Simetrik Anahtar Şifreleme Yöntemleri				
	Symmetric Key Encryption Methods				
5	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Özüt Çıkarma Yöntemleri				
	Extraction Methods				

6	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Blok Şifreleme Yöntemleri				
	Block Cipher Methods				
7	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Ara Sınav				
	Midterm Exam				
8	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	RSA				
	RSA				
9	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Sayısal İmza				
	Digital Signature				
10	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Sayısal İmza				
	Digital Signature				
11	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Anahtar Dağıtımı				
	Key Distribution				

12	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Anahtar Kararlaştırma				
	Key Decisioning				
13	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Sır Dağıtım Yöntemleri				
	Secret Distribution Methods				
14	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Genel Tekrar				
	General Review				

DEĞERLENDİRME / EVALUATION

Yarıyıl (Yıl) İçi Etkinlikleri / Term (or Year) Learning Activities	Sayı / Number	Katkı Yüzdesi / Percentage of Contribution (%)
Ara Sınav / Midterm Examination	1	100
Toplam / Total:	1	100
Başarı Notuna Katkı Yüzdesi / Contribution to Success Grade(%):		40

Yarıyıl (Yıl) Sonu Etkinlikleri / End Of Term (or Year) Learning Activities	Sayı / Number	Katkı Yüzdesi / Percentage of Contribution (%)
Final Sınavı / Final Examination	1	100
Toplam / Total:	1	100
Başarı Notuna Katkı Yüzdesi / Contribution to Success Grade(%):		60

Etkinliklerinin Başarı Notuna Katkı Yüzdesi(%) Toplamı / Total Percentage of Contribution (%) to Success Grade:	100
Değerlendirme Tipi / Evaluation Type:	

İŞ YÜKÜ / WORKLOADS

Etkinlikler / Workloads	Sayı / Number	Süresi (Saat) / Duration (Hours)	Toplam İş Yüğü (Saat) / Total Work Load (Hour)
Ara Sınav / Midterm Examination	1	72.00	72.00
Ara Sınav İçin Bireysel Çalışma / Individual Study for Mid term Examination	1	1.00	1.00
Final Sınavı / Final Examination	1	76.00	76.00
Final Sınavı için Bireysel Çalışma / Individual Study for Final Examination	1	1.00	1.00
Toplam / Total:	4	150.00	150.00
Dersin AKTS Kredisi = Toplam İş Yüğü (Saat) / 25.00 (Saat/AKTS) = 150.00/25.00 = 6.00 ~ 6.00 / Course ECTS Credit = Total Workload (Hour) / 25.00 (Hour / ECTS) = 150.00 / 25.00 = 6.00 ~ 6.00			

PROGRAM VE ÖĞRENME ÇIKTISI / PROGRAM LEARNING OUTCOMES

Öğrenme Çıktıları / Learning Outcomes	Program Çıktıları / Program Outcomes														
	1.1.1	1.1.2	1.1.3	1.1.4	1.1.5	1.1.6	1.1.7	1.1.8	1.1.9	1.1.10	1.1.11	1.1.12	1.1.13	1.1.14	1.1.15
1.Öğrenciler, bilgisayar sistemlerini etkileyebilecek çeşitli güvenlik tehditlerini tanıyacak ve analiz edeceklerdir. / Students will recognize and analyze various security threats that can affect computer systems.	5	4	4	5	4	4	4	4	5	4	4	4	5	5	4
2.Öğrenciler, şifreleme teknikleri ve algoritmalarını anlayarak, verilerin güvenliğini sağlamak için kriptografiyi etkili bir şekilde uygulayabileceklerdir. / By understanding encryption techniques and algorithms, students will effectively apply cryptography to ensure data security.	4	4	5	4	4	5	5	5	4	3	4	4	3	4	4
3.Öğrenciler, güvenli ağlar oluşturmak ve ağ tabanlı saldırılara karşı korunmak için gerekli stratejileri geliştireceklerdir. / Students will learn network security principles to develop necessary strategies for creating secure networks and protecting against network-based attacks.	4	4	5	5	5	4	4	4	4	4	5	4	3	4	5
4.Öğrenciler, kuruluşlar için etkili güvenlik politikaları geliştirmek ve uygulamak için gereken bilgiyi kazanacaklardır. / Students will gain the knowledge required to develop and implement effective security policies for organizations.	4	3	4	4	4	5	4	5	3	4	5	4	4	4	5

5.Öğrenciler, yazılım ve sistemlerdeki güvenlik açıklarını tespit etme yeteneklerini geliştirerek, bu açıkları kapatmak için etkili savunma stratejileri oluşturabileceklerdir. / By enhancing their ability to identify security vulnerabilities in software and systems, students will create effective defense strategies to address these vulnerabilities.	4	4	4	4	4	5	5	4	5	5	4	5	5	4	5
--	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Katkı Düzeyi / Contribution Level : 1-Çok Düşük / Very low, 2-Düşük / Low, 3-Orta / Moderate, 4-Yüksek / High, 5-Çok Yüksek / Very high