GENEL TANIM / GENERAL DESCRIPTION

Ders Adı / Course Name	Crypto-Systems and Cryptographic Protocols / Crypto-Systems and Cryptographic Protocols	
Ders Kodu / Course Code	9105055232019	
Ders Türü / Course Type		
Ders Seviyesi / Course Level	Second Cycle / Second Cycle	
Ders Akts Kredi / ECTS	8.00	
Haftalık Ders Saati (Kuramsal) / Course Hours For Week (Theoretical)	3.00	
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	Face to Face / Face to Face	
Eğitim Dili / Education Language	Turkish / Turkish	
Ön Koşulu Olan Ders(ler) / Precondition Courses	Yok	None
Amacı / Purpose	Bu dersin amacı öğrencilerin; paylaşılmış ve açık anahtarlı kriptografi temellerinin kavramasını ve güvenlik uygulamalarında kriptografik protokollerden hangisini ve/veya hangilerini kullanabileceğine karar vermesini sağlamaktır.	The objectives of this course includes helping students develop: - Understanding of the fundamentals of shared and public key cryptography. - Ability to select the appropriate cryptographic protocols for a given security application.
İçeriği / Content	Klasik şifreleme yöntemleri, yerine koyma, Permütasyon, Playfair, Vigenere, Kusursuz Gizlilik ve Tek kullanımlık şifre, DES, Açık anahtarlı şifreleme yöntemleri, RSA, El-Gamal, Kimlik Doğrulama ve Dijital İmza protokolleri, kriptosistemlerde protokol zayıflıkları, Kuantum Kriptografi.	Classical Ciphers, Substitution, Permutation, Playfair, Vigenere, Perfect secrecy and one-time pad, Data Encryption Standard, Public Key Cryptography, RSA, El-Gamal, Diffie-Hellman key exchange, Authentication and Digital Signature, Bit Commitment and Fair Coin Flips, Zero-knowledge Proofs, Protocol failures in cryptosystems, Quantum cryptography.
Önerilen Diğer Hususlar / Recommended Other Considerations	Yok	None
Staj Durumu / Internship Status	Yok	None
Kitabı / Malzemesi / Önerilen Kaynaklar / Books / Materials / Recommended Reading	Paar and Pelzl, Understanding Cryptography, Springer, 2010 Stinson, Douglas R., Cryptography: Theory and Practice, CRC Press, 1995 Schneier, B., Applied Cryptography, 2/e, Wiley, 1996 CrypTool http://www.cryptool.de/	Paar and Pelzl, Understanding Cryptography, Springer, 2010 Stinson, Douglas R., Cryptography: Theory and Practice, CRC Press, 1995 Schneier, B., Applied Cryptography, 2/e, Wiley, 1996 CrypTool http://www.cryptool.de/
Öğretim Üyesi (Üyeleri) / Faculty Member (Members)	Prof.Dr. Mehmet Emin DALKILIÇ	

ÖĞRENME ÇIKTILARI / LEARNING OUTCOMES

1	Mantıksal, analitik ve soyut düşünebilme.	Logical, Analytical and Abstract Reasoning
2	Bilgi sistemlerinin değişik katmanlarında, kriptografik protokolleri uygulayabilme (Kimlik tespiti, Yetkilendirme, İletişim güvenliği, Mesaj gizliliği, Gönderici ve Alıcının gizliliği, mesaj bütünlüğü, doğrulama, vs.)	Ability to apply cryptographic protocols at various layers of Information Systems (Identification, Authorization, Communication Security, Message Confidentiality, Sender and Receiver Secrecy, Message Integrity and authentication)
3	Güvenlik protokollerinin zayıf noktalarını tespit edebilme.	Ability to do an Vulnerabiliy Analysis on Security Protocols
4	Anahtar oluşturma, dağıtımı ve değişimi sürecinde kullanılan yöntemleri uygulayabilme.	Abilty to carry on the processes used at key establishment, distribution and key exchange
5	Kriptografik sistemler alanında araştırma yapıp sunabilme.	Ability to do reseach and present the results realted to cryptography

HAFTALIK DERS İÇERİĞİ / DETAILED COURSE OUTLINE

Hafta / Week					
1	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Kriptografiye Giriş Basit şifreleme yöntemleri (Yerine koyma, Permütasyon, Vigenere)	İnternet Tarama			
	Inroduction to Cryptıgraphy, Historical Ciphers				
2	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Akış Şifreleme	Okuma, Ödev			
	Stream Ciphers				
3	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	DES Veri Şifreleme standardı	İnternet Tarama			
	DES Data Encryption Standard				
4	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	AES İleri Şifreleme Standardı	Okuma, Ödev			
	AES Advanced Encryption Standard				
5	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Blok Şifreleme İleri Konular	İnternet Tarama			
	More About Block ciphers				

6	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Açık anahtarlı şifreleme yöntemleri ve matematiksel temelleri	Okuma, Ödev			
	Introduction to Public Key Cryptography				
7	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	RSA Şifreleme Sistemi	İnternet Tarama			
	RSA Encryption System				
8	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Arasınav				
	Midterm Exam				
9	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Ayrık Logaritma Tabanlı Şifreleme Sistemleri	İnternet Tarama, Ödev			
	Discrete Logarithm Based Encryption Systems				
10	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Eliptik Eğri Kriptografisi	Okuma			
	Elliptic Curve Cryptography				
11	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
	Bit Commitment and Fair Coin Flips, Zero-knowledge Proofs	İnternet Tarama, Ödev			

	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
12	Sayısal İmza Protokolleri	Okuma			
	Digital Signarure Protocols				
	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
13	Kriptografik Öz ve MAC fonksiyonları	İnternet Tarama, Ödev			
	Cryptographic Hash and MAC Functions				
	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
14	İleri Kriptografik Protokoller (Bit Adama, Adil Yazı-Tura, Sıfır Bilgi Kanıtları vb.)	Dönem Projesi Sunumları			
	Advanced Cryptograpic Protocols (Bit Commitment, Fair Coin-Flips, Zero Knowledge Proofs)				
	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
15	Proje Sunumları	Dönem Projesi Sunumları			
	Project Presentations				
	Teorik Dersler / Theoretical	Uygulama	Lab	Öğretim Yöntem ve Teknikleri/Teaching Methods Techniques	Ön Hazırlık / Preliminary
16	Final Sınavı				
	Final Exam				

DEĞERLENDİRME / EVALUATION

Yarıyıl (Yıl) İçi Etkinlikleri / Term (or Year) Learning Activities	Sayı / Number	Katkı Yüzdesi / Percentage of Contribution (%)
Ara Sınav / Midterm Examination	1	38
Proje Hazırlama / Project Preparation	1	31
Ev Ödevi / Homework	1	31
Toplam / Total:	3	100
Başarı Notuna Katkı Yüzdesi / Contribution to Success Grade(%):		65

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(%):		35

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 Yükü (Saat) / Total Work Load (Hour)
Ara Sınav / Midterm Examination	1	2.00	2.00
Final Sınavı / Final Examination	1	2.00	2.00
Derse Katılım / Attending Lectures	14	3.00	42.00
Proje Hazırlama / Project Preparation	1	50.00	50.00
Bireysel Çalışma / Self Study	7	2.00	14.00
Ödev Problemleri için Bireysel Çalışma / Individual Study for Homework Problems	6	5.00	30.00
Ara Sınav İçin Bireysel Çalışma / Individual Study for Mid term Examination	1	30.00	30.00
Final Sınavı içiin Bireysel Çalışma / Individual Study for Final Examination	1	40.00	40.00
Okuma / Reading	5	3.00	15.00
Toplam / Total:	37	137.00	225.00

Dersin AKTS Kredisi = Toplam İş Yükü (Saat) / 30.00 (Saat/AKTS) = 225.00/30.00 = 7.50 ~ / Course ECTS Credit = Total Workload (Hour) / 30.00 (Hour / ECTS) = 225.00 / 30.00 = 7.50 ~

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.Mantıksal, analitik ve soyut düşünebilme. / Logical, Analytical and Abstract Reasoning	4		3	1		4	4
2.Bilgi sistemlerinin değişik katmanlarında, kriptografik protokolleri uygulayabilme (Kimlik tespiti, Yetkilendirme, İletişim güvenliği, Mesaj gizliliği, Gönderici ve Alıcının gizliliği, mesaj bütünlüğü, doğrulama, vs.) / Ability to apply cryptographic protocols at various layers of Information Systems (Identification, Authorization, Communication Security, Message Confidentiality, Sender and Receiver Secrecy, Message Integrity and authentication)	4				1	3	2
3.Güvenlik protokollerinin zayıf noktalarını tespit edebilme. / Ability to do an Vulnerabiliy Analysis on Security Protocols	3	2				3	2
4.Anahtar oluşturma, dağıtımı ve değişimi sürecinde kullanılan yöntemleri uygulayabilme. / Abilty to carry on the processes used at key establishment, distribution and key exchange	4				1	3	2
5.Kriptografik sistemler alanında araştırma yapıp sunabilme. / Ability to do reseach and present the results realted to cryptography	5	5	2	1		4	3

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