İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Eliptik Eğriler ile Kriptografi	Cryptography with Elliptic Curves

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
	Guz/Bahar	3	7.5	YL (M.Sc.)

Lisansüstü Program (Graduate Program)	Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography)		
Dersin Türü (Course Type)	Seçmeli (Elective)	**Dersin Dili (Course Language)**	İngilizce English

Dersin İçeriği **(Course Description)** *30-60 kelime arası*	Eliptik Eğri grupları. Eliptik eğri grupları içinde hesaplama. Eliptik Eğri Kriptografi. Weil/Tate çiftleri. Kimliğe Dayalı Şifreleme. El Gamal algoritmaları. Eliptik eğriler ile çarpanlarına ayırma. Elliptic Curve Groups. Computing in elliptic curve groups. Elliptic curve cryptography. Weil/Tate pairings. Identity based encryption. El Gamal algorithms. Factorization with elliptic curves.
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	1. Eliptik eğri temelli şifreleme ve şifre çözme algoritmalarını anlamak ve analiz etmek için yeterli matematiksel altyapı hazırlamak. 2. Öğrencileri eliptik eğri temelli şifreleme alanında zorlu problemlere hazırlamak. 3. Veri paylaşma ve veri transferi konularında güvenli metotlar öğretmek. 1. To provide sufficient mathematical background to understand and analyze encryption/decryption algorithms based on elliptic curves. 2. To prepare the students for the challenging problems in the area of elliptic curves cryptography. 3. To teach secure methods for data sharing and data transferring.
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	1. Weil/Tate çiftleri algoritmalarını gerçekleştirebilmek. 2. Eliptik eğri grupları içinde hesaplama için algoritmalar gerçekleştirebilmek. 3. Bilinen pairing tabanlı şifreleme politikalarını gerçekleştirebilmek. 4. Eliptik eğri üzerine şifreleme ve şifre çözme politikalarının kripto analizini yapabilmek. 5. Eliptik eğri üzerine şifreleme algoritmaları gerçekleştirip uygulayabilmek. 6. Eliptik eğri grupları için çarpanlarına ayırma problemini öğrenmek A Msc/PhD student completing this course successfully should 1. Be able to implement Weil/Tate pairing algorithms. 2. Ben able to implement algorithms for computing in elliptic curve groups. 3. Be able to construct and execute known pairing based encryption schemes. 4. Be able to make cryptanalysis of encryption/decryption schemes based on elliptic curves. 5. Be able to implement/execute current cryptographic algorithms based on elliptic curves. 6. Be able to use elliptic curve groups for factoring integers.

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*	1) H. Cohen, G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC Press, 2005. 2) L. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd edition 2008. 3) J. Katz, Y. Lindell, Introductıon to Modern Cryptography: Principles and Protocols, Chapman & Hall/CRC, 2007. 4) A. Menezes, P. C. Van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.		
Ödevler ve Projeler **(Homework & Projects)**	**7 HOMEWORKS AND 2 PROJECTS**		
Laboratuar Uygulamaları **(Laboratory Work)**	**7 RECITATION IN COMPUTER LAB**		
Bilgisayar Kullanımı **(Computer Use)** *Dersinizde kullnadığınız yazılım ve simulasyon programları yazılabilir*	**C, C++, MATHEMATICA, PARI, SAGE. MAGMA.** **C, C++, MATHEMATICA, PARI, SAGE, MAGMA.**		
Diğer Uygulamalar **(Other Activities)**			
Başarı Değerlendirme Sistemi **(Assessment Criteria)**	**Faaliyetler (Activities)**	**Adedi* (Quantity)**	**Değerlendirmedeki Katkısı, % (Effects on Grading, %)**
	Yıl İçi Sınavları (Midterm Exams)	**1**	**20%**
	Kısa Sınavlar (Quizzes)		
	Ödevler (Homework)	**7**	**30%**
	Projeler (Projects)	**2**	**10%**
	Dönem Ödevi/Projesi (Term Paper/Project)		
	Laboratuar Uygulaması (Laboratory Work)		
	Diğer Uygulamalar (Other Activities)		
	Final Sınavı (Final Exam)	**1**	**%40**

*****Yukarıda Belirtilen Sayılar Minimum Olup Yerine Getirilmesi Zorunludur.

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Eliptik eğri üzerine genel bilgiler: Eliptik Eğri Grubu	2
2	Eliptik eğri üzerine genel bilgiler: Weil ve Tate Çiftleri	1, 2
3	Çiftler tabanlı Şifreleme: Kimliğe Dayalı Şifreleme	1, 2, 3, 4, 5
4	Çiftler tabanlı Şifreleme: Kimliğe Dayalı Şifreleme	1, 2, 3, 4, 5
5	Çiftler tabanlı Şifreleme: Özelliğe Dayalı Şifreleme	1, 2, 3, 4, 5
6	Çiftler tabanlı Şifreleme: Coppersmith Metodu	1, 2, 3, 4, 5
7	Çiftler tabanlı Kripto analiz	1, 2, 4
8	Koblitz Eliptik Eğri Algoritması	2, 4, 5
9	Diffie-Hellman Anahtar Değişimi	2, 4, 5
10	Massey-Omura Şifreleme	2, 4, 5
11	ElGamal Açık Anahtarlı Şifreleme	2, 4, 5
12	ElGamal Dijital İmza Algoritması	2, 4, 5
13	Eliptik Eğri Açık Anahtarlı Şifreleme	2, 4, 5
14	Eliptik Eğri ile çarpanlarına ayırma	2, 6

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Background on Elliptic Curves: Elliptic Curve Group	2
2	Background on Elliptic Curves: Weil and Tate Pairing	1, 2
3	Pairing Based Cryptography: Identity Based Encryption	1, 2, 3, 4, 5
4	Pairing Based Cryptography: Identity Based Encryption	1, 2, 3, 4, 5
5	Pairing Based Cryptography: Attribute Based Encryption	1, 2, 3, 4, 5
6	Pairing Based Cryptanalysis: Coppersmith's Method	1, 2, 3, 4, 5
7	Pairing Based Cryptanalysis: MOV Attack	1, 2, 4
8	Koblitz's Elliptic Curve Algorithm	2, 4, 5
9	Diffie-Hellman Key Exchange	2, 4, 5
10	Massey-Omura Encryption	2, 4, 5
11	ElGamal Public Key Encryption	2, 4, 5
12	ElGamal Digital Signature Algorithm	2, 4, 5
13	Elliptic Curve Public Key Algorithm	2, 4, 5
14	Factoring using Elliptic Curves	2, 6

NOT-1: Ders planı, sadece hafta bazında işlenen ders konularını içermeli, ara ve kısa sınavlar ders planlarına yazılmamalıdır.

Dersin Bilgi Güvenliği Mühendisliği Yüksek Lisans Programıyla İlişkisi

	Programın mezuna kazandıracağı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, Bilgi Güvenliği ve Kriptografi alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi).			X
ii.	Bilgi Güvenliği ve Kriptografi alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).			X
iii.	Bilgi Güvenliği Kriptografi alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).			X
iv.	Bilgi Güvenliği ve Kriptografi alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).		X	
v.	Bilgi Güvenliği ve Kriptografi alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (beceri).		X	
vi.	Bilgi Güvenliği ve Kriptografi alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
vii.	Bilgi Güvenliği ve Kriptografi alanı ile ilgili uygulamalarda karşılaşılan ve öngörülemeyen karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilme ve sorumluluk alarak çözüm üretebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
viii.	Bilgi Güvenliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
ix.	Bilgi Güvenliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).		X	
x.	Bilgi Güvenliği ve Kriptografi alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde Türkçe ve/veya İngilizce olarak aktarabilme (İletişim ve Sosyal Yetkinlik).			
xi.	Sosyal ilişkileri ve bu ilişkileri yönlendiren normları eleştirel bir bakış açısı ile inceleyebilme, geliştirebilme ve gerektiğinde değiştirmek üzere harekete geçebilme (İletişim ve Sosyal Yetkinlik).			
xii.	Bilgi Güvenliği ve Kriptografi alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			X
xiii.	Bilgi Güvenliği ve Kriptografi alanı ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamalarında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilme ve bu değerleri öğretebilme (Alana Özgü Yetkinlik).			
xiv.	Bilgi Güvenliği ve Kriptografi alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).			
xv.	Bilgi Güvenliği ve Kriptografi alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).			
xvi.	Kendi çalışmalarını, Bilgi Güvenliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).			

1: Az, 2. Kısmi, 3. Tam

Relationship between the Course and Information Security Engineering Graduate (MS) Curriculum

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in Information Security and Cryptography area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).			X
ii.	Grasping the inter-disciplinary interaction related to Information Security and Cryptography area (knowledge).			X
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in Information Security and Cryptography area (skill).			X
iv.	Interpreting and forming new types of knowledge by combining the knowledge from Information Security and Cryptography area and the knowledge from various other disciplines (skill).		X	
v.	Solving the problems faced in Information Security and Cryptography area by making use of the research methods (skill).		X	
vi.	The ability to carry out a specialist study related to Information Security and Cryptography area independently (Competence to work independently and take responsibility).			
vii.	Developing new strategic approaches to solve the unforeseen and complex problems arising in the practical processes of Information Security and Cryptography area and coming up with solutions while taking responsibility (Competence to work independently and take responsibility).			
viii.	Fulfilling the leader role in the environments where solutions are sought for the problems related to Information Security Cryptography area (Competence to work independently and take responsibility)			
ix.	Assessing the specialist knowledge and skill gained through the study with a critical view and directing one's own learning process (Learning Competence).		X	
x.	Systematically transferring the current developments in Information Security and Cryptography area and one's own work to other groups in and out of Information Security Engineering area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency).			
xi.	Ability to see and develop social relationships and the norms directing these relationships with a critical look and the ability to take action to change these when necessary. (Communication and Social Competency).			
xii.	Using the computer software together with the information and communication technologies efficiently and according to the needs of Information Security and Cryptography area (Communication and Social Competency).			X
xiii.	Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Information Security and Cryptography area related data and the ability to teach these values to others (Area Specific Competency).			
xiv.	Developing strategy, policy and application plans concerning the subjects related to Information Security and Cryptography ng area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency).			
xv.	Using the knowledge and the skills for problem solving and/or application (which are processed within the area) in inter-disciplinary studies (Area Specific Competency).			
xvi.	The ability to present one's own work within the international Information Security and Cryptography environments orally, visually and in written forms (Area Specific Competency).			

1: Little, 2. Partial, 3. Full

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***
Enver Özdemir		